Health Matrix: The Journal of Law-Medicine

Volume 10 | Issue 1 Article 9

2000

DNA Database Statutes & Privacy in the Information Age

Warren R. Webster, Jr.

NOTE

DNA DATABASE STATUTES & PRIVACY IN THE INFORMATION AGE

Warren R. Webster, Jr.[†]

I. INTRODUCTION

The human body is the best picture of the human soul.[1]

ALTHOUGH WRITTEN WELL BEFORE the advent of deoxyribonucleic acid (DNA) technology, these words seem increasingly to reflect reality with each passing day. The concept of genetic identity presents new constitutional questions never imagined before Watson and Crick discovered the double-helix. These issues concern privacy and whether it can be protected in the age of The Human Genome Project.[2]

The ability to collect and analyze DNA samples is a breakthrough for medical science and law enforcement, but it

---

† J.D., Case Western Reserve University School of Law, 1999.

[1] HENRY LE ROY FINCH, WITTGENSTEIN 142 (1995) (quoting LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS, 178 (G.E.M. Anscombe & R. Rhees eds., G.E.M. Anscombe trans., Oxford: Blackwell 1953)).

[2] The Human Genome Project (HGP), also known as the Human Genome Initiative, is a federally funded attempt to map the entire human genome in order to identify and eradicate all genetically based disease. *See generally* George P. Smith & Thaddeus J. Burns, *Genetic Determinism or Genetic Discrimination?*, 11 CONTEMP. HEALTH L. & POL'Y 23, 29-32 (1994). The HGP had initial funding of 135 million dollars. It is estimated that the project will cost three billion dollars and be completed in 2005. *See* Roberta M. Berry, *The Human Genome Project and the End of Insurance*, 7 U. FLA. J. L. & PUB. POL'Y 205, 206 (1996) (citing Daniel Kelves, *Out of Eugenics: The Historical Politics of the Human Genome*, *in* THE CODE OF CODES: SCIENTIFIC AND SOCIAL ISSUES IN THE HUMAN GENOME PROJECT 3, 36 (Daniel J. Kelves & Leroy Hood eds., 1992) and Victor A. McKusic, *The Human Genome Project: Plans, Status, and Applications in Biology and Medicine*, *in* GENE MAPPING: USING LAW AND ETHICS AS GUIDES 18, 18 (George J. Annas & Sherman Elias eds., 1992)).

also presents a threat to the American notions of autonomy and the right to privacy. In the past decade, state legislatures have authorized the collection and analysis of DNA from certain types of criminal offenders to "assist federal, state and local criminal justice and law-enforcement agencies in the identification . . . or prosecution of violent crimes, sex-related crimes, and other crimes against the person,"[3] and to deter recidivist acts.[4] The DNA is analyzed, in the form of a DNA fingerprint or profile, digitized, and retained for later identification purposes in a DNA databank.[5] These databanks then serve primarily as an informational tool for law enforcement personnel, allowing them to match DNA evidence recovered from crime scenes with the profiles stored in the databanks. State databases are nationally linked through a federal system called the Combined DNA Identification System (CODIS).[6]

The federal and state governments are not unaware of privacy concerns surrounding DNA databanks. The National Research Council states:

> Confidentiality and security of DNA-related information are especially important and difficult issues, because we are in the midst of two extraordinary technological revolutions that show no signs of abating: in molecular biology, which is yielding an explosion of information about human genetics, and in computer technology, which is moving toward national and international networks connecting growing information resources.[7]

Thus, most states have included privacy provisions in their statutes authorizing the creation of DNA databanks and imposing

---

[3] W. VA. CODE § 15-2B-2 (1998).

[4] *See, e.g.*, LA. REV. STAT. ANN. § 15:602 (West Supp. 1999); IOWA CODE ANN. § 13.10 (West 1995); *see generally* NATIONAL RESEARCH COUNCIL, DNA TECHNOLOGY IN FORENSIC SCIENCE 119 (1992) (providing statistical data on recidivism rates of prisoners released in eleven states in 1983).

[5] Although "databank" and "database" are often used interchangeably, databank means a repository of actual DNA samples while database refers to a DNA record system. *See generally* IDAHO CODE § 19-5502 (9)-(10) (1997). In this Note, I will also use "databank" and "database" interchangeably to generically refer to statutes authorizing the collection, storage, and testing of DNA samples, and otherwise note the distinction where important.

[6] *See* discussion *infra* Part IV.D (describing CODIS and some of its privacy protection measures).

[7] NATIONAL RESEARCH COUNCIL, *supra* note 4, at 113-14.

sanctions for proscribed acts concerning DNA samples and DNA information. The question then is whether or not DNA database statutes adequately address privacy concerns.

The purpose of this Note is to study the measures state legislatures have adopted to address privacy concerns and determine if their DNA database statutes are sufficient to protect privacy. Part II briefly describes the science underlying DNA and DNA profiling. Part III provides a history of the challenges to non-consensual DNA collection and the use of DNA evidence. Finally, Part IV presents a critical analysis of current DNA databank statutes, argues that legislatures have neglected privacy by failing to address the fate of DNA samples.

II. THE SCIENCE OF DNA ANALYSIS

The science surrounding molecular genetics is difficult, if not impossible, for the uninitiated to understand. It is not surprising, therefore, that the issues of DNA collection, storage, and use in many aspects of our society leave us unsure of whether our privacy has been breached or is in jeopardy. A basic understanding of DNA science provides some foundation for a constitutional analysis.

A. DNA

There are approximately 100 trillion cells in the human body.[8] Each cell processes its own amino acids, simple carbohydrates, lipids, and trace elements into proteins, complex lipids, carbohydrates, and nucleic acid.[9] Chromosomes, which are structures of DNA and protein-carrying hereditary material, are contained in these cells. Each nucleated cell contains twenty-two pairs of autosomes, or non-sex chromosomes, and two sex chromosomes: XX for females, XY for males. At inception, half of the twenty-three chromosomal pairs are supplied by the mother and half by the father. Chromosomes contain a double-helix structure called DNA. DNA consists of a chain of nucleic acids or nucleotides in various sequences. The types of DNA nucleotides are adenine (A), guanine (G), cytosine (C), and thymine (T). The nucleotides of each strand bond with their counterpart to form the double helix: C-to-G, A-to-T. A se-

[8] *See* ANDRE A. MOENSSENS ET AL., SCIENTIFIC EVIDENCE IN CIVIL AND CRIMINAL CASES 879-80 (4th ed. 1995).

[9] *See id.* at 880.

quence of three nucleotides, called a codon, forms an amino acid. The genetic code is read by identifying amino acids. A gene, therefore, is a series of codons read in a series from a fixed starting point.[10] Genes, which transmit inherited traits, are specific sequences of nucleotides at certain chromosomal locations called loci. Some genes may consist of several thousand base-pairs of nucleotides. Others may consist of more that one million.

The DNA molecule is found in all cells which have a nucleus, such as sperm cells, white blood cells, bone marrow cells, cells found in saliva, and cells surrounding hair roots.[11] The entire genetic code, or genome, of an individual is contained in each cell nucleus and is identical in each cell. Each strand of the DNA double-helix consists of alternating phosphate and sugar (deoxyribose) groups. Because the individual nucleotides bond to the deoxyribose groups in random order, there is "tremendous potential for variation[s]."[12]

These variations give each human, except for identical twins, unique DNA. For this reason, DNA is a helpful tool for law enforcement officials. Collectable samples of DNA are contained in bodily fluids such as blood, semen, and saliva.[13] DNA can also be extracted from sweat, nasal secretions, and teeth.[14] Over ninety-nine percent of the approximately three billion base pairs are the same among humans, leaving about three million base pairs which vary.[15] DNA typing thus focuses on the segments of DNA that are highly variable, called "polymorphic" sites or loci. DNA typing allows scientists to find differences, deletions, and insertions as small as one nucleotide.[16]

---

[10] *See* BENJAMIN LEWIN, GENES IV 68 (1990) (discussing the basic structure of DNA).

[11] *See* MOENSSENS ET AL., *supra* note 8, at 881.

[12] *Id.* at 884.

[13] *See* Yale H. Yee, Note, *Criminal DNA Data Banks: Revolution for Law Enforcement or Threat to Individual Privacy?*, 22 AM. J. CRIM. L. 461, 464 (1995) (citing Eric Lander, *DNA Fingerprinting: Science, Law, and the Ultimate Identifier*, *in* THE CODE OF CODES 191, 192 (Leroy Hood & Daniel J. Kevles eds., 1992)).

[14] 2 PAUL C. GIANNELLI & EDWARD J. IMWINKLERIED, SCIENTIFIC EVIDENCE 2 n.1.1 (2d ed. Supp. 1998) (citations omitted) (noting the different means of obtaining DNA).

[15] 2 PAUL C. GIANNELLI & EDWARD J. IMWINKLERIED, SCIENTIFIC EVIDENCE § 18-2, at 2 (2d ed. 1993).

[16] *See* Yee, *supra* note 13.

B. Determining a Match

Although DNA provides all the information pertaining to an individual's physical traits, DNA "fingerprinting" does not utilize this vast amount of information.[17] Instead, by using variations at specific loci, DNA samples can be compared against one another to determine similarities or the lack thereof. Thus, DNA fingerprinting involves a comparison of samples, and subsequently, the probability of a match. A determination is made by a human examiner, often with the help of a computerized system, as to whether different samples originate from the same source, different sources, or whether the test is inconclusive. A number of genetic tests are available, including: multi and single locus restriction fragment-length polymorphism-based typing (RFLP) and polymerase chain reaction-based typing (PCR), including direct sequencing. PCR-based typing is generally considered superior to RFLP-based typing because it requires a smaller sample and can be accomplished in less time.

Despite the typing method used, critics have challenged the statistics of determining a match. In terms of privacy, the question of whether the accuracy of DNA typing alone call for a wider test population is raised. As one author explains: "The great number of possible alleles (or possible variants) at each highly polymorphic site has greatly complicated the task of collecting adequate data necessary to calculate the probability that any allele would occur in a wide population."[18] Others contend that current theoretical models and procedures are sufficient to compensate for errors, if any, resulting from subpopulation variations, and that the debate on this is essentially resolved,[19] a view which may cause once skeptical courts to change their position on DNA admissibility.[20]

---

[17] *See* Dan L. Burke & Jennifer A. Hess, *Genetic Privacy: Constitutional Considerations in Forensic DNA Testing*, 5 GEO. MASON U. CIV. RTS. L. J. 1, 4 (1994).

[18] Kenneth R. Kreiling, *DNA Technology in Forensic Science*, 33 JURIMETRICS J. 449, 455 (1993).

[19] However, it is argued that even with the current sample population, statistical estimates compensate for the scope of the testing population and do not lead to erroneous results. *See* Eric S. Lander & Bruce Budowle, *DNA Fingerprinting Dispute Laid to Rest*, 371 NATURE 735, 736-37 (1994) (claiming that conservative estimates used to calculate match probabilities negate the effects population substructure has on such estimates).

[20] *See* MOENSSENS ET AL., *supra* note 8, § 15.17.

III. CHALLENGES TO THE USE OF DNA EVIDENCE & COLLECTION

A. Admissibility of DNA Evidence

In the United States, DNA fingerprinting was first admitted into evidence in 1988.[21] As a fledgling science, DNA fingerprinting had to overcome state and federal standards regarding its admissibility. DNA evidence has been admitted under both the *Frye v. United States*[22] and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*[23] tests.[24] As time passes, the admissibility of DNA evidence under both *Frye*'s "general acceptance test" and the more liberal *Daubert* standard increases. First, although *Daubert* is binding only in federal courts, it is influential in state courts, especially those that have adopted the Federal Rules of Evidence.[25] Many states have even taken legislative steps to ensure the admissibility of DNA evidence and probability.[26] Now, as one commentator states, "DNA evidence is admissible in every state and federal circuit--in one form or the

---

[21] *See* Yee, *supra* note 13, at 465-66 (discussing Andrews v. State, 533 So.2d 841 (Fla. Dist. Ct. App. 1988), and United States v. Yee, 129 F.R.D. 629 (N.D. Ohio 1990)).

[22] 293 F. 1013 (D.C. Cir.1923) (holding that in order for a scientific theory or principle to be introduced into evidence, it must have gained general acceptance in its field).

[23] 509 U.S. 579 (1993) (holding that under Rule 702 of the Federal Rules of Evidence the trial judge must determine "that an expert's testimony both rests on a reliable foundation and is relevant to the task at hand").

[24] *See generally* Brian Huseman, Note, *Taylor v. State, Rule 706, and the DNA Database: Future Directions in DNA Evidence*, 22 OKLA. CITY U. L. REV. 397, 410-18 (1997) (discussing *Frye* and *Daubert*, and their application to DNA evidence).

[25] *See* Jennifer Sue Deck, *Prelude to a Miss: A Cautionary Note Against Expanding DNA Databanks in the Face of Scientific Uncertainty*, 20 VT. L. REV. 1057, 1078 (1996) (citing William C. Thompson, *Evaluating the Admissibility of New Genetic Identification Tests: Lessons from the "DNA War,"* 84 J. CRIM. L. & CRIMINOLOGY 22, 32 (1993)). "[D]NA profiling procedures are capable of being tested and have been tested, although in a non-blind setting. [T]he process has been subjected to peer review and publication, and both the Office of Technology Assessment and the National Research Council have endorsed the general reliability of RFLP profiling. [Finally], most courts have held that questions concerning the rate of error go to the weight, instead of the admissibility, of the evidence." *Id.* at 1077-78 (citations omitted).

[26] *See* MOENSSENS ET AL., *supra* note 8, § 15.20 (noting that a number of states have legislatively recognized the reliability of DNA typing through a number of ways, such as eliminating the need for an expert witness to testify that DNA analysis is trustworthy and dependable). *See, e.g.*, ALA. CODE § 36-18-30 (1997) (requiring expert DNA testimony to be admissible if it meets *Daubert* standards).

other."[27] The growing reliability and increased use of DNA information invariably increases the importance of issues surrounding the collection and storage of DNA information.

B. Collection of DNA

DNA profiling is greatly facilitated by the ability to collect and store profiles and samples for future retrieval. Because of this, state legislatures have authorized the creation of DNA databanks. DNA databases provide a repository of genetic records, which law enforcement officials can use for criminal identification purposes.[28] These samples are generally gathered from invasive bodily extractions, most commonly blood samples. The Supreme Court recognizes that such non-consensual blood extractions implicate the Fourth Amendment.[29]

Many citizens argue that the collection of genetic material in this manner violates our basic notions of privacy and thus, the constitutionality of statutes authorizing the collection of DNA samples have been challenged. A variety of legal attacks have been mounted under the Fourth Amendment right to be free from "unreasonable searches and seizures," the Fifth and Fourteenth Amendments' "due process" clauses, the Article I "*ex post facto*" law prohibition, and the Eighth Amendment's "cruel and unusual punishment" clause.[30] However, courts have held that statutes authorizing non-consensual DNA extraction do not violate the Constitution on a number of grounds.

---

[27] Paul C. Giannelli, *The DNA Story: An Alternative View*, 88 CRIM. L. & CRIMINOLOGY 380, 380-81 (1997) (reviewing Harlan Levy's book, AND THE BLOOD CRIED OUT).

[28] *See* Michael J. Markett, Note, *Genetic Diaries: An Analysis of Privacy Protection in DNA Databanks*, 30 SUFFOLK U. L. REV. 185 (1996).

[29] *See* Schmerber v. California, 384 U.S. 757, 767 (1966) (stating that non-consensual blood sample extraction "plainly involves the broadly conceived reach of a search and seizure under the Fourth Amendment"); *see also* Skinner v. Railway Labor Executives' Association, 489 U.S. 602, 616 (1989) (stating that physical intrusion, penetrating the skin, infringes on reasonable privacy expectations).

[30] *See* Rise v. Oregon, 59 F.3d 1556 (9th Cir. 1995) (challenging an Oregon statute on unreasonable search and seizure, and due process grounds); Vanderlinden v. Kansas, 874 F. Supp. 1210 (D. Kan. 1995) (challenging a Kansas statute on unreasonable search and seizure, due process, *ex post facto*, and equal protection grounds); State v. Olivas, 856 P.2d 1076 (Wash. 1993) (arguing that a Washington statute violates the prohibition on unreasonable searches and the grant of equal protection, and is unconstitutionally vague).

First, the procedure is generally deemed "minimally intrusive."[31] Courts have held that DNA collection, like fingerprinting, constitutes a routine booking procedure.[32] Thus, once a person is in the lawful custody of the state, DNA collection is an identification procedure and constitutionally distinct from the collection of blood from "free persons."[33] Courts have found this to be related to the legitimate state interest in ascertaining the identity of suspects. "[T]he identification of suspects is relevant not only to solving the crime for which the suspect is arrested, but also for maintaining a permanent record to solve other past and future crimes."[34]

Second, prisoners have diminished rights of privacy.[35] The Fourth Circuit in *Jones v. Murray* was first to apply this concept to the statutorily mandated collection of DNA for data banking purposes. It found, simply, that "[w]ith [a] person's loss of liberty upon arrest comes the loss of at least some, if not all, rights to privacy otherwise protected by the Fourth Amendment."[36]

Similarly, the argument that such statutes violate the *ex post facto* clause of the Constitution[37] has been dismissed. The Ninth Circuit has stated that "[a] law implicates the Ex Post Facto Clause only if it criminalizes conduct that was not a crime when it was committed, increases the punishment for a crime beyond what it was at the time the act was committed, or deprives a person of a defense available at the time the act was committed."[38] Thus, laws requiring felons to submit blood samples for DNA databanks do not raise *ex post facto* concerns, even if such statutes were passed after a prisoner has been incarcerated.[39] In accordance, prisons may adopt reasonable

---

[31] *See* People v. Wealer, 636 N.E.2d 1129, 1136 (Ill. App. Ct. 1994); *see also* Rise, 59 F.3d at 1559.

[32] *See* Rise v. Oregon, 59 F.3d at 1560.

[33] *Id.*

[34] Jones v. Murray, 962 F.2d 302, 306 (4th Cir. 1992) (upholding Virginia statute requiring convicted felons to provide blood samples for DNA analysis).

[35] *See id.* (explaining that persons lawfully arrested on probable cause and detained by the state do not have the same protections as free persons).

[36] *Id.*

[37] U.S. CONST. Art I, § 10, cl. 1 (stating that "[n]o State shall...pass any...ex post facto Law...").

[38] *Rise*, 59 F.3d at 1562 (citing Collins v. Youngblood, 497 U.S. 37, 42-43 (1990)).

[39] *See Jones*, 962 F.2d at 309 (finding that a requirement of a DNA sample is not punitive in nature and that its sole purpose is to help establish a databank that will aid future law enforcement).

regulations to enforce compliance with DNA databank statutes even if they allow punishment for non-compliance.[40]

Finally, courts have dismissed the argument that forceful submission to DNA collection procedures violates a prisoner's right to be free from cruel and unusual punishment. In *Kruger v. Ericson*,[41] the court found that "[a]lthough there is no static 'test'" to determine cruel and unusual punishment, the application of the Eighth Amendment must come from society's maturing "standards of decency."[42] Finding that the drawing of blood was conducted by a trained technician, in accordance with medically acceptable procedures, the court concluded that "[t]he use of a needle is hardly the cruel and unusual punishment contemplated by the Eighth Amendment."[43]

Although DNA collection and use is widely accepted, further constitutional challenges are likely if DNA databases expand in scope to encompass larger populations. Because offenses covered under databanking laws varies among the states, the boundries of DNA databanks remains unsettled.

IV. DNA DATABANK DANGERS

A. Scope of DNA Databanks

Currently, all fifty states have laws establishing forensic DNA databases.[44] Many original databanking fears surrounded

---

[40] *See id.* (concluding that prison regulations and their enforcement are contemplated at the original sentencing, and thus do not classify as additional punishment).

[41] 875 F. Supp. 583 (D. Minn. 1995).

[42] *Id.* at 587 (citing Rhodes v. Chapman, 452 U.S. 337, 346 (1981)).

[43] *Id.* at 588 (quoting Boreland v. Vaughn, No. CIV.A.92-1072, 1993 WL 62707 (E.D.Pa. 1993), *aff'd*, 22 F.3d 300 (3rd Cir. 1994)).

[44] *See* ALA. CODE § 36-18-20 (Michie Supp. 1998); ALASKA STAT. ANN. § 44.41.035 (1998); ARIZ. REV. STAT. ANN. § 31-281 (West 1989), § 13-4438 (West Supp. 1998); ARK. CODE ANN. §§ 12-12-1105, -1106 (1999); CAL. PENAL CODE ANN. § 295 (Deering Supp. 1999); COLO. REV. STAT. ANN. § 17-2-201(5)(g)(I) (1998); CONN. GEN. STAT. ANN. § 54-102g (West Supp. 1999); DEL. CODE ANN. § 4713 (1997); FLA. STAT. ANN. § 943.325 (West 1997); GA. CODE ANN. § 24-4-60 (1995); HAW. REV. STAT. § 706-603 (1993 & Supp. 1999); IDAHO CODE § 19-5505 (1997 & Supp. 1999); 730 ILL. COMP. STAT. ANN. 5/5-4-3 (West 1993 & Supp. 1999); IND. CODE § 10-1-9-8 (West 1982); IOWA CODE ANN. §§ 13.10 (West 1995); IOWA ADMIN. CODE r. 61-8.1(13) (1998); KAN. STAT. ANN. § 21-2511 (1995 & Supp. 1998); KY. REV. STAT. ANN. § 17.170 (Banks-Baldwin 1999); LA. REV. STAT. ANN. §§ 15: 605, 606 (West Supp. 1999); ME. REV. STAT. ANN. tit. 25, § 1571 (West 1988 & Supp. 1998); MD. ANN. CODE OF 1957 art. 88B, § 12A (Michie Butterworth 1995 & Supp. 1997); MASS. GEN LAWS ANN. ch. 22E, § 2 (West Supp. 1999); MICH. COMP. LAWS

the timing of DNA sample extraction. It was unclear whether DNA database statutes would mandate collection from mere suspects. Now, all DNA statues appear to be triggered only after a conviction. Cases like *Rise v. Oregon*[45] once previewed a future in which DNA samples would be taken from virtually all criminal suspects. But this has not been the trend of state legislatures. Now, all DNA database statutes appear to be triggered only after conviction. While the timing of sample extraction is settled, the scope of these laws is uncertain.

Many statutes authorize collection only from sex offenders. Others encompass a larger population of criminals, sometimes including crimes that are not likely to yield DNA evidence. For example, Idaho mandates collection, not only for sexual abuse, rape, and murder, but also for robbery, aggravated arson, and even racketeering.[46] North Carolina includes, among others, the burning of a mobile home and the malicious throwing of corrosive acid or alkali in their list of crimes covered by the state DNA databank law.[47] The range of crimes covered under database statutes has increased, and continues to do so, from the original purpose of detecting and curbing sexually related crimes.[48]

ANN. § 750.520m (West 1991 & Supp. 1999); MINN. STAT. ANN. §§ 609.3461, 299C.155 (West Supp. 1999); MISS. CODE ANN. § 45-33-15 (West 1999); MO. ANN. STAT. §§ 650.050, .055 (West Supp. 1999); MONT. CODE ANN. § 44-6-102 (1999); NEB. REV. STAT. § 29-4104 (Supp. 1998); NEV. REV. STAT. § 176.0913 (1998); N.H. REV. STAT. ANN. § 632-A:21 (LEXIS Supp. 1999); N.J. STAT. ANN. § 53:1-20.21 (West Supp. 1999); N.Y. EXEC. LAW § 995-c (McKinney 1996); N.C. GEN. STAT. § 15A-266.4, .5 (1997); N.D. CENT. CODE § 31-13-05 (1996); OHIO REV. CODE ANN. § 2901.07 (Baldwin 1994 & Supp. 1999); OKLA. STAT. ANN. tit. 57, § 588 (West Supp. 1999); *id.* tit. 74, § 150.27 (West 1995 & Supp. 1999); OR. REV. STAT. §§ 181.085, 137.076 (1997); PA. STAT. ANN. tit. 35, § 7651.301 (West Supp. 1999); R.I. GEN. LAWS § 12-1.5-4 (LEXIS Supp. 1998); S.C. CODE ANN. § 23-3-610 (West Supp. 1997); S.D. CODIFIED LAWS § 23-5-14 (1998); TENN. CODE ANN. § 38-6-113 (1997), § 40-35-321 (1997 & Supp. 1999); TEX. GOV'T. CODE ANN. § 411.142 (West 1998); UTAH CODE ANN. § 53-10-406 (LEXIS Supp. 1999); VT. STAT. ANN. tit. 20, § 1933 (1997 & Supp. 1999); VA. CODE ANN. § 19.2 - 310.2 (Supp. 1999); WASH. REV. CODE ANN. § 43.43.752 (West 1998); W. VA. CODE § 15-2B-4 (Michie 1995 & Supp. 1999); WIS. STAT. ANN. §§ 165.76-77, 973.047 (West 1998); WYO. STAT. ANN. § 7-19-402 (1999).

[45] 59 F.3d 1556 (noting a state's interest in identifying suspects).

[46] *See* IDAHO CODE § 19-5506 (1997).

[47] *See* N.C. GEN. STAT. § 15A-226.4 (1997).

[48] *See* Jean E. McEwen & Phillip R. Reilly, *A Review of State Legislation on DNA Forensic Data Banking*, 54 AM. J. HUM. GENETICS 941, 944-45 (1994).

B. Do Databanks Work?

The evidence suggests that database statutes are producing intended results in homicide and sex-offender crimes. For example, Virginia's database recently produced a "match," despite the lack of a suspect,[49] in the murder of Hope Denise Hall.[50] Florida's DNA databank had produced eighty-seven matches by 1997,[51] and 155 "cold hit" matches by November of 1998.[52] Other states have also had similar success with their databanks.[53] The national database, CODIS, also appears to be an effective weapon in fighting sex crimes. It produced matches that led to arrests almost immediately after operation commenced.[54] According to the F.B.I, the national databank has produced more than 400 matches.[55] Despite the current and anticipated success of DNA databanks, protests concerning the dangers of DNA databanking have not ceased.

C. Information Privacy

With these statutes, the legislatures have attempted to address privacy concerns. Most DNA database statutes provide penalties for wrongfully obtaining or disseminating protected DNA information.[56] But, as some researchers argue, "many states, in their rush to create databanks, have paid little attention

---

[49] This is sometimes referred to as a "cold hit."

[50] *See Search of Database Leads to "Cold Hit" Arrest in 1994 Slaying*, THE VIRGINIA PILOT & THE LEDGER STAR, Jan. 9, 1997, *available in* 1997 WL 6390445 (discussing an arrest made based on a DNA match of the arrestee's blood with semen found at the crime scene).

[51] *See* Jackie Hallifax, *DNA Databases Open Cold Cases: Genetic Fingerprints Give Law Enforcers Hot Weapon*, DAILY REC. (Baltimore), Sept. 22, 1997, at 25A.

[52] *See* Jeremy Manier & Steve Mills, *DNA Policy Kept Suspect Free*, CHI. TRIB., Oct. 18, 1998, at 19.

[53] *See, e.g.*, Dan Morain, *Genetic Sleuthing*, L.A. TIMES, Feb. 20, 1997, at A3 (describing California's DNA criminal profile project); Kathy Walt, *DNA Database to Identifies Suspect*, HOUSTON CHRON., Sept. 10, 1998, at 19A.

[54] *See* Jesse Garza, *DNA Leads to Arrest in 3 Rapes: New Database Links Suspects to Years-Old Attacks in UW-Parkside Area*, MILWAUKEE J.-SENTINEL, Oct. 20, 1998, *available in* WL 14045802 (noting that the suspect was identified and arrested two days after national F.B.I. database opened).

[55] *See FBI Launches National DNA Profile Index*, AGENCE FRANCE PRESSE, Oct. 14, 1998, *available in* LEXIS, News Library, News Group File.

[56] *But see, e.g.*, KAN. STAT. ANN. § 21-2511 (1995 & Supp. 1998) (failing to address unlawful dissemination or use of DNA information); OR. REV. STAT. § 181.085 (1997) (limiting disclosure of DNA information and transfer of DNA samples, but not under threat of sanctions).

to issues of quality control, quality assurance, and *privacy*."[57] DNA databanking privacy issues can be divided into two major categories: (1) confidentiality of DNA profiles and (2) the disposition of DNA samples. Most legislation addresses DNA profiles, but ultimately neglects to address adequately privacy issues concerning the DNA samples.[58] Ambiguities often remain as to whether a state will store samples and, if so, for how long.

Sanctions for violations of DNA database statutes vary. For example, the Oklahoma statute simply states that "[a]ny person charged with the custody and dissemination of information from the database shall not divulge or disclose any such information except to federal, state, county or municipal law enforcement or criminal justice agencies."[59] Conviction under this section constitutes a misdemeanor, punishable by imprisonment for not more than one year.[60] In New Jersey, "[a]ny person who by virtue of employment, or official position . . . purposely discloses" individually identifiable DNA information to unauthorized sources is guilty of a disorderly persons offense.[61] A violation in Massachusetts can bring a maximum $1000 fine or six-month incarceration.[62] The South Carolina statute reads: "A person who willfully discloses . . . DNA information contained in the State DNA Database to . . . [those] not entitled to receive this information is guilty of a misdemeanor . . . ."[63] It is also a misdemeanor to obtain willfully such information.[64] The South Carolina statute is typical of confidentiality provisions in that it authorizes only the results of DNA profiling tests to be released to federal, state, and local law enforcement agencies.[65] Thus, there are widespread prohibitions restricting DNA information dissemination, of both DNA profiles and DNA samples, at the

---

[57] *See* McEwen & Reilly, *supra* note 48, at 957 (emphasis added).

[58] *See* discussion *infra* Part IV.G.-I.

[59] OKLA. STAT. ANN. tit. 74, § 150.27a (West 1995 & Supp. 1999). The statute also exempts DNA database information from any statute requiring disclosure of information to the public and makes such information inadmissible in civil court proceedings.

[60] *See id.*

[61] N.J. STAT. ANN. § 53:1-20.26 (West Supp. 1999).

[62] *See* MASS. GEN. LAWS ANN. ch. 22E, § 12 (West Supp. 1999).

[63] S.C. CODE ANN. § 23-3-650(B) (West Supp. 1999).

[64] *See id.* § 23-3-650(C).

[65] *See id.* § 23-3-650(A).

state level. The restrictions placed on access to DNA information is reinforced nationally by federal law.[66]

D. The National System

Databases from the various states are linked to each other through a system called the Combined DNA Identification System (CODIS). Congress granted the Federal Bureau of Investigation (FBI) the power to establish an index of DNA profiles under the DNA Identification Act of 1994 (the Act).[67] CODIS carries its own privacy protection standards and criminal penalties. A fine of not more than $100,000 is levied for knowingly disclosing or obtaining unauthorized individually identifiable data.[68] Additionally, access to CODIS is subject to cancellation if certain measures designed to protect privacy are not recognized by criminal justice agencies.[69] The legislatures, in jurisdictions wishing to use CODIS, are charged with developing rules for their own databanks which adhere to those in the statute.[70] States have adopted these parameters in their respective statutes, but this, as I will discuss, does not ensure that our constitutional notions of privacy will be protected.

E. The Future

It is not difficult to imagine that persons other than criminals will be required to submit DNA samples for other governmental interests. Many statutes already provide that data obtained from DNA analysis, albeit anonymous, be made available to various officials for purposes other than law enforcement.[71]

---

[66] *See* discussion *infra* Part IV.D (describing the DNA Identification Act and the implications it has for the individual states).

[67] *See* 42 U.S.C.A. § 14132(a) (West 1995).

[68] *See* 42 U.S.C.A. § 14133(c) (West 1995).

[69] *See* 42 U.S.C.A. § 14132(c) (West 1995).

[70] *See* 42 U.S.C.A. § 14132(b) (West 1995) (maintaining that federal, state, and local criminal justice agencies be subject to rules which limit information disclosure only: to criminal justice agencies for law enforcement purposes; in judicial proceedings, if permitted; for criminal defense purposes; for population statistics databases, if identifiable information is removed; and for protocol, research, and quality control purposes).

[71] *See, e.g.*, OHIO REV. CODE ANN. § 109.573 (Baldwin Supp. 1999) (allowing DNA database information to be used in determining the existence of parent-child relationships); TEX. GOV'T CODE ANN. § 411.143 (West 1998) (allowing the DNA database to be used for the identification of living or deceased missing persons and human remains from a disaster).

These statutes recognize the potential value of a more encompassing DNA databank. For instance, many states authorize anonymous DNA information to be disseminated for, among others, quality control purposes and population statistics databases.[72]

The National Research Council has already asserted, without disclosing identifying information, that "[a]ny population databank used to support forensic DNA typing should be openly available for reasonable scientific inspection . . . . According to long-standing and wise scientific tradition, the data underlying an important scientific conclusion must be freely available."[73] As the ability to collect, analyze, and use DNA information increases, more calls for expanding the scope and uses of databanks may be inevitable. The advantages of DNA identification and information systems are not limited to criminal justice purposes. For instance, public health may one day be enhanced through wide-spread screening for predisposition to a number of diseases. Similarly, many states have already implemented DNA databases to assist in the identification of human remains from natural or mass disasters, or to identify unidentified persons.[74]

Some observers have argued that DNA databanks should encompass a larger population than just criminals, to include the entire general public.[75] Still other commentators have advocated other national uses for DNA, such as for identification in health-care settings.[76] The Department of Defense requires blood samples from all military personnel for the purpose of identifying remains, should the need arise. However, it appears unlikely that such a national system will be accepted anytime soon. The prevailing consensus, as noted by the National Research Council,[77] dictates against widespread use in the civilian population. The Council cautions against moving in the direction of expanded databases because "Americans have generally

---

[72] *See id.*

[73] N.E. Norton, *The Forensic DNA Endgame*, 37 JURIMETRICS J. 477, 493 (1997) (quoting the National Research Council's first report on DNA evidence);.

[74] *See, e.g.*, ALA. CODE § 36-18-24 (1997).

[75] *See* NATIONAL RESEARCH COUNCIL, *supra* note 4, at 121 (addressing the opinion that, because many in the general public are already required to be fingerprinted for security and identification purposes, the same rationale could be used in support of DNA profiles).

[76] *See infra* note 80.

[77] *See* NATIONAL RESEARCH COUNCIL, *supra* note 4, at 122.

been reluctant to allow the creation of national identification systems, and DNA profiling poses a special risk of invasion of privacy (concerning personal and medical traits)."[78] But what information do DNA databases and databanks put at risk?

F. What Information Can DNA and DNA Fingerprints Provide?

Many commentators have noted that a DNA fingerprint contains little or no genetic information.[79] This is so because RFLP analysis focuses on junk regions of DNA. These regions "do not appear to contain either coding sequences or genetic control sequences."[80] Thus, currently, a banding pattern can only be used for identification purposes. The DNA fingerprint itself yields no additional genetic information. In order for a banding pattern to produce more information, DNA probes need to be developed for those particular traits. Furthermore, "whether these traits are determined by one gene, a combination of genes, or some interaction between genes and the individual's environment is not known at this time."[81]

Hugh Miller, III, cautions that our genetic information does not constitute the "Holy Grail" of personal identity and thus deserves no more legal protection than other types of medical information.[82] This point is well-taken in a healthcare provider-patient context. But where the government mandates collection of DNA and retains control over the information contained therein, the provisions for privacy protection must be scrutinized carefully. "It is important that the law realize it is simply not a matter of what we can currently read from the DNA profile analysis, but what we will be able to read from this genetic

---

[78] *Id.*

[79] *See generally* JoAnn M. Longobardi, Note, *DNA Fingerprinting and the Need for a National Data Base*, 17 FORDHAM URB. L. J. 323 (1989).

[80] Lisa L. Dahm, *Using DNA Profile as the Unique Patient Identifier in the Community Health Information Network: Legal Implications*, 15 J. MARSHALL J. COMPUTER & INFO. L. 227, 256 (1997) (arguing for the use of DNA fingerprints as "patient" identifiers in the context of healthcare services) (quoting Dan L. Burk, *DNA Identification Testing: Assessing the Threat to Privacy*, 24 U. TOL. L. REV. 87, 94 (1992)).

[81] *Id.* at 258 (quoting Arno G. Motulsky, *Societal Problems of Forensic Use of DNA Technology*, DNA TECH. & FORENSIC SCI. 3, 5 (1989).

[82] *See* Hugh Miller, III, *DNA Blueprints, Personhood, and Genetic Privacy*, 8 HEALTH MATRIX 179, 180-81 (1998) (arguing that "advances to genetic science cannot warrant any transformation of the traditional idea of personal identity into essentially genetic terms").

information in the very near future."[83] Although a person's DNA may not be the "sacred vessel"[84] of an individual's personality, it does contain potentially sensitive information which can have negative effects for the donor if not properly protected, now and in the future.

DNA databases which retain only test results and destroy the sample would not pose a serious threat to privacy. The FBI's computerized system for compiling DNA profiles from the various states contains only the results of a test, not the actual sample.[85] Thus, the federal government will not "retain samples of blood, hair, semen, or other fluid from which the DNA is extracted for testing."[86] What the various states may do with the DNA samples is another question.

In the rush to create DNA databases, many states have failed to resolve thoroughly privacy issues.[87] For states that have provided sanctions for infractions that jeopardize a donor's privacy, a question still remains as to whether the penalties imposed will be sufficient in the future in light of the inevitable increase in value of DNA information. Since a DNA profile has only limited potential to facilitate invasions of privacy, it appears that most legislatures have taken the necessary precau-

---

[83] E. Donald Shapiro & Michelle L. Weinberg, *DNA Databanking: The Dangerous Erosion of Privacy*, 38 CLEV. ST. L. REV. 455, 472 (1990).

[84] Miller, III, *supra* note 82, at 221 (arguing that "DNA information should no more be conflated with the 'sacred vessel' of an individual's inviolate personality than should ordinary medical information about his blood type or white cell count").

[85] *See* Nicholas Wade, *F.B.I. Set To Open Its DNA Database For Fighting Crime*, N.Y. TIMES, Oct. 12, 1998, at A1. Wade states that:

> Under a new DNA profiling system known as S.T.R.s, for short tandem repeats, a person's DNA is tested at 13 specific sites at which a short length of DNA is repeated .... The number of repeats is highly variable ... [and] gives a way of identifying each individual with a probability of one in several billion .... All that goes into the computerized DNA databases is the set of 13 numbers from the S.T.R. measurements. Only identifying information, and nothing about a person's health or appearance, can be divined from the S.T.Rs.

Id.

[86] Manning A. Conners, III, Comment, *DNA Databases: The Case for the Combined DNA Index System*, 29 WAKE FOREST L. REV. 889, 895 (1994) (citing *Forensic DNA Analysis: Joint Hearing on H.521-24 Before the House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, and the Senate Committee on the Judiciary, Subcommittee on the Constitution*, 102d Cong., 2d Sess. 21, 22 (1991)).

[87] *See generally* McEwen & Reilly, *supra* note 48, at 956 (noting that only a few states mandate criminal penalties for unauthorized disclosure or use of DNA data).

tions to protect this limited data. Most states have not failed to address privacy concerns associated with DNA profiles and even samples under their prohibition clauses. However, unique privacy concerns surround the fate of actual DNA samples.

G. The Threat

The greatest threat to individual privacy comes from the ambiguity in state statutes regarding the fate of DNA samples. Many state legislatures have failed to codify clear rules governing the fate of the actual sample after it has been tested.[88] For example, Florida law provides that the "Department of Law Enforcement shall . . . [r]eceive, process, and store blood samples and the data derived therefrom furnished pursuant to subsection (1)."[89] However, subsection (1) only specifies that two specimens of blood be submitted by persons convicted of enumerated offenses to designated testing facilities.[90] Typically, DNA database laws simply prescribe DNA profile results to be maintained in a database, without mention of the actual DNA samples.[91] The disposition of DNA samples is left to designated state agencies, often with little or no guidance.[92] Even CODIS, the FBI system linking state databases, provides no direction as to the fate of DNA samples.[93] In fact, federal law, through CODIS, contemplates that states will store DNA samples, but does not provide direction concerning the duration of time that sample retention would be acceptable.[94]

---

[88] *See, e.g.*, FLA. STAT. ANN. § 943.325 (West 1997) (discussing only what will be done with the results of the analysis and not the fate of the sample itself).

[89] *Id.* § 943.325(7).

[90] *See id.* § 943.325(1).

[91] *See, e.g.*, GA. CODE ANN. § 24-4-60 (1995) (providing that "[t]he identification characteristics of the profile resulting from the DNA analysis shall be stored and maintained by the bureau in a DNA data bank"); HAW. REV. STAT. ANN. § 706-603 (1993 & Supp. 1999); IOWA CODE ANN. § 13.10 (West 1995); MASS. GEN. LAWS ANN. ch. 22E (West Supp. 1999).

[92] *See, e.g.*, S.C. CODE ANN. § 23-3-640 (West Supp. 1999) (leaving the disposition of all DNA samples at the discretion of the South Carolina Law Enforcement Division); ALASKA STAT. ANN. § 44.41.035(h) (1998) (designating that "[t]he Department of Public Safety shall adopt reasonable procedures (1) for the collection, analysis, storage, expungement, and use of the DNA registration system").

[93] *See* 42 U.S.C.A. § 14132(b) (West 1995) (stating that "[t]he index shall include only information on DNA identification records and DNA analyses that are . . . (3) maintained by Federal, State, and local criminal justice agencies pursuant to the rules that allow disclosure of *stored DNA samples* . . .") (emphasis added).

[94] *See id.*

Still, other states explicitly,[95] or implicitly,[96] authorize the indefinite storage of DNA samples of known and unknown donors. The National Research Council's cryptic recommendations reflect the difficulties states face when writing DNA databank laws. The Council writes:

> *In general, the committee discourages the retention of DNA samples.* However, there is a practical reason to retain DNA samples for short periods. Because DNA technology is changing so rapidly, we expect the profiles produced with today's methods to be incompatible with tomorrow's methods. Accordingly, today's profiles will need to be discarded and replaced with profiles based on the successor methods. It would be extremely expensive and inefficient to have to redraw blood samples for retyping. *We are therefore persuaded that retention of samples after typing should be permitted for the short term--only during the startup phase of DNA profile databanks.* As databanks become established and technology stabilizes somewhat, samples should be destroyed promptly after typing.[97]

---

[95] *See, e.g.*, LA. REV. STAT. ANN. § 15: 606 (West Supp. 1999) (establishing a state DNA databank to "serve as the repository of DNA samples collected under this Chapter"); N.J. STAT. ANN. § 53:1 - 20.21 (West Supp. 1999) (providing that "[t]he DNA sample itself will be stored in the State DNA databank"); MD. CODE ANN. OF 1957 art. 88B, § 12A(f) (Michie Butterworth 1995 & Supp. 1997) (stating that "[t]he DNA sample shall be stored and maintained by the Crime Laboratory in the statewide DNA repository"); MINN. STAT. ANN. § 299C.155 (West Supp. 1999) (stating that "[t]he Bureau shall adopt uniform procedures and protocols to maintain, *preserve*, and analyze human biological specimens for DNA") (emphasis added); OKLA. STAT. ANN. tit. 74, § 150.27a(A) (West 1995 & Supp. 1999) (establishing an offender database "for the purpose of collecting and *storing* blood samples," and analyzing and typing of genetic markers) (emphasis added); OR. REV. STAT. § 181.085(a) (1997) (authorizing the Department of State Police to store blood samples).

[96] *See, e.g.*, DEL. CODE ANN. tit. 29, § 4713(i) (1997) ("A person whose DNA profile has been included in the [Delaware] DNA databank . . . may petition . . . for expungement on the ground that the conviction . . . has been reversed or dismissed. The [state] shall expunge all identifiable information pertaining to the person and destroy all samples from the person upon receipt of a certified court order."); WYO. STAT. ANN. §§ 7-19-402(b), -404(c) (1999) (referencing DNA samples which are "collected and stored"); N.D. CENT. CODE § 31-13-07 (1996) (mandating the destruction of "all samples" from a person who has successfully petitioned the court for expungement).

[97] NATIONAL RESEARCH COUNCIL, *supra* note 4, at 122 (emphasis added).

States that have addressed, or will address, the issue face the problem of defining the parameters of the startup phase of DNA profile databanks. Without this knowledge or the ability to predict, state legislatures are faced with the problem of having to destroy samples in order to quell threats to privacy, only to have the profiling basis change. "[W]e doubt that existing RFLP-based technology provides a wise long-term foundation for such a databank. We expect current methods to be replaced soon with techniques that are simpler, easier to automate, and less expensive but incompatible with existing DNA profiles."[98] In fact, new and more simple techniques are now available in the form of PCR-based profiles. However, there is little indication that PCR technology will not be surpassed by a better system, as was RFLP.

Of the few states that have adequately addressed privacy concerns associated with DNA samples, only one state, Wisconsin, explicitly mandates the destruction of a DNA sample after DNA profiling results have been obtained.[99] Virginia's DNA database statute impliedly does not allow its state agencies to retain DNA samples after profiling.[100] Furthermore, both Virginia[101] and Wisconsin[102] have prohibitions specifically dealing with DNA samples. A few states, like Indiana, legislate that samples may not be "stored for the purpose of obtaining information about human physical traits or predisposition for disease."[103] The attempts to limit the purposes for which DNA can be used is a step in the right direction but does not end the privacy debate. The question of whether such legislation will suffice to protect privacy concerns, now and in the future, still remains.

---

[98] *Id.* at 129.

[99] WIS. STAT. ANN. §§ 165.77(2), (3), 973.047(1) (West 1998) (providing that blood specimens should be destroyed following analysis and conclusion of all applicable court proceedings).

[100] VA. CODE ANN. § 19.2 - 310.2 (Supp. 1999) (providing requirements for DNA analysis).

[101] *Id.* § 19.2 - 310.6 (1995) (stating that "[e]xcept as authorized by law, any person who, for purposes of having DNA analysis performed, obtains or attempts to obtain any sample submitted to the Division of Forensic Science for analysis shall be guilty of a Class 5 felony").

[102] WIS. STAT. ANN. § 165.77(5) (West 1998) (stating that "[a]ny person who intentionally disseminates a specimen received under this section . . . in a manner not authorized . . . may be fined not more than $500 or imprisoned for not more than 30 days or both").

[103] IND. CODE § 10-1-9-18 (West Supp. 1999).

H. Lessons From the Past

A number of potential problems, from inadvertent disclosure to fraud, arise when citizens are required to surrender personal information for safekeeping by the government. The inherent dangers in collecting DNA samples have been noted.[104] The legislative history of this country suggests that promises to protect privacy are only temporary. For instance, Social Security numbers were originally intended to be used for the limited purposes contained in the Social Security Act.[105] Today, Social Security numbers are a primary means of governmental and private sector identification. In the private sector, Social Security numbers are used for identification by financial and educational institutions as well as for blood donations and medical records. Governmental sources use these numbers for, among other things, tax and employment purposes, law enforcement, driving records, child support, professional licensing, and student loans.[106] Government employees with access to these Social Security numbers have illegally accessed this information to sell the numbers for financial gain.[107] Some have argued that entities motivated by profit and self-interest, such as insurance companies and health maintenance organizations, will attempt to obtain information stored in genetic profiles as a precondition of coverage.[108]

One commentator argues that "penalties for misusing DNA samples and information should be strictly enforced in order to prevent and deter any potential for misuse that may remain."[109] The protection of privacy is undoubtedly aided through the en-

---

[104] *See* Shapiro & Weinberg, *supra* note 83, at 473-84 (discussing the effects of DNA databanking on privacy).

[105] *See id.* at 477-78 (citations omitted).

[106] *See* Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529 (1998) (discussing the many uses of Social Security numbers and the problems associated with such uses).

[107] *See id.* at 534 (citations omitted).

[108] *See* Shapiro & Weinberg, *supra* note 83, at 482. *See generally* Natalie Anne Stepanuk, *Genetic Privacy and Third Party Access to Information: New Jersey's Pioneering Legislation as a Model for Federal Privacy Protection of Genetic Information*, 47 CATH. U. L. REV. 1105 (1998) (arguing that as genetic data becomes more available, insurance companies will base premiums on the degree of genetic flaws — something that obviously calls for an increase in testing and widespread access).

[109] Connors, *supra* note 86, at 908 (discussing the North Carolina DNA Database Act of 1993, as it was the first tailored after suggested federal legislative guidelines).

forcement of prohibition clauses in DNA database statutes. However, it is the potential for misuse, fostered by legislative uncertainty regarding DNA samples, which presents the greatest threat.

I. A Databank Proposal

The easily imagined expansion of the scope of DNA databanks and the ever increasing information which genetics yields is a legitimate cause for concern when analyzing current DNA databank statutes. Because DNA information contains unknown potential to expose many aspects of human life, laws designed to protect confidentiality must counterbalance this massive potential. Inadequate laws, even if strictly enforced, will not stop the encroachment on privacy. States should discourage indefinite retention of DNA samples after DNA profiling by providing more guidance concerning the disposition of samples to the appropriate agencies. To accommodate both the evolving DNA technology and privacy concerns, states could set specific time limits on the retention of DNA samples. After a designated amount of time, based on a reasonable estimate of when the "startup" phase[110] will end, profiled samples should be destroyed. This differs from the National Research Council's current recommendation[111] in that it requires a logistical risk. The suggestion to wait and destroy DNA samples only after typing technology "stabilizes" is a concept too elusive to protect privacy concerns. A firm, but reasonable, time limit constitutes a necessary measure to strike a balance between law enforcement and the civil liberty concerns associated with governmental storage of DNA samples.

V. CONCLUSION

Ultimately, DNA databanks will continue to prove extremely effective to law enforcement ends. The most effective databank would, obviously, contain as many samples as possible, and would retain the actual biological sample for future developments in DNA testing. This efficiency, however, would come at a price that is, the retention of DNA samples by governmental entities and the growing ability to decipher one's genetic code. Although the federal and state governments have

---

[110] *See supra* text accompanying note 97.

[111] *See id.*

mandated anonymity in non-criminal contexts such as statistical health data sharing, the potential for abuse or even mistake concerning DNA samples, coupled with the growing information DNA yields, is a threat primarily because states have failed to address the fate of DNA samples.

Although DNA might not provide the key to unlocking the human personality, it does contain information that could be damaging to donors because of the unknown potential as an indicator for other aspects of human life, from behavior to disease. For this reason, provisions governing the fate of DNA samples require the utmost effort to ensure that our notions of privacy are protected. First, DNA use should be restricted to the original criminal identification purpose. Second, unauthorized distribution, acquisition, tampering, and use of DNA samples and results should continue to be sufficiently sanctioned, and thus discouraged.[112] Finally, states should set mandatory dates for DNA sample destruction.

What secrets future DNA analysis holds is unknown and difficult to predict. What abuses may accompany the warehousing of such secrets is easier to foresee. All that can be done in the "information age,"[113] where knowledge increasingly equates to power, is demand that our legislatures recognize the potential threats to fundamental American concepts of privacy when ushering in new technologies. Accordingly, many states need to reassess their DNA database laws and decide specifically the fate of DNA samples.

---

[112] As DNA information may prove to be more and more valuable, states should amend their sanctions for illegal dissemination to reflect this.

[113] ALVIN TOFFLER, POWER SHIFT: KNOWLEDGE, WEALTH, AND VIOLENCE AT THE EDGE OF THE 21ST CENTURY 9 (1990) (describing how the economy has come to rely on the transfer and use of information, rather than on manual labor).