Bioethical Objections to DNA Databases for Law Enforcement: Questions and Answers

D.H. Kaye[*]

Every state now stores information about the DNA of people convicted of crimes.[1] These databases help police to solve cases that had baffled them for decades[2] and to catch previously convicted offenders who commit new crimes.[3] Examples abound. In Virginia, there was the rapist who blew out a candle before attacking his victim. The candle had his saliva. There was the burglar who wore a pair of socks on his hands and left no fingerprints. The discarded socks contained skin cells. There was the bank robber who dropped his ski mask. All were identified by checking the DNA profiles in these traces against the state's database of convicted felons.[4]

Yet, amassing DNA samples and data is becoming intensely controversial. The state and federal databases have been said to "taint

---

[*] Regents' Professor, Arizona State University College of Law; Fellow, Center for the Study of Law, Science, and Technology. This article is adapted from remarks presented at the National Institute of Justice's Fourth Annual Conference on the Future of DNA: Implications for the Criminal Justice System, Albuquerque, May 1999, and the annual meeting of the Association of American Law Schools' Section on Law and Medicine, San Francisco, January 2001.

[1] *See* Robin Cheryl Miller, Annotation, *Validity, Construction, and Operation of State DNA Database Statutes*, 76 A.L.R.5th 239 (2000).

[2] *See, e.g.*, Associated Press, *DNA Allegedly Ties Florida Inmate to '80 O.C. Rape-Murder*, L.A. TIMES, Apr. 20, 2001, at B4; C.J. Chivers, *DNA Match Implicates Inmate in '79 Murder, Officials Say*, N.Y. TIMES, Mar. 13, 2000, at B1; Melita Marie Garza, *DNA Database Helps Track '89 Rape Suspect*, CHICAGO TRIB., Dec. 10, 1997, at 12, *available at* 1997 WL 36199382; Bryan Smith, *DNA Puts Its First Rapist Away*, PORTLAND OREGONIAN, Jan. 12, 1996, *available at* 1996 WL 4099349.

[3] There are many other sources of DNA samples that law enforcement officials might wish to examine in specific cases. Many samples are held by hospitals, public health authorities, health maintenance organizations, biomedical researchers, and the military. *See generally* STORED TISSUE SAMPLES: ETHICAL, LEGAL, AND PUBLIC POLICY IMPLICATIONS (Robert A. Weir ed., 1998). Access to the samples in these non-law enforcement repositories, for the purpose of criminal investigations or prosecutions, is discussed in Edward J. Imwinkelried & D.H. Kaye, *DNA Typing: Emerging or Neglected Issues*, 76 WASH. L. REV. 413 (2001).

[4] *See* PROFILE: USE OF A DNA DATA BANK TO CATCH CRIMINALS IN VIRGINIA (Nat'l Public Radio broadcast, Mar. 8, 2001), *available at* 2001 WL 9326731.

justice"[5] by "unfettered government-sponsored bioinvasion,"[6] and to be part of a "surveillance creep"[7] and "the dangerous erosion of privacy."[8] This Article surveys the ethical objections that have been made to DNA databanking.[9] Although the objections vary in their merit, all raise issues that must be addressed in designing DNA databanks for law enforcement.[10]

I. OF DATABANKS AND DATABASES

To address the various criticisms, it is important to understand what DNA databanking does—and does not—involve. As currently practiced in almost all jurisdictions, a sample of blood, saliva, or other tissue or fluid is collected from a convicted offender, a fraction is taken for analysis, and the remainder is preserved and stored. A minute portion of the genetic information in the subsample is analyzed. The analysis generally is limited to thirteen locations, or *loci*, that yield patterns, or *genotypes*, that approach the level of unique identification. These genotypes, expressed as a set of numbers, are entered into local and state databases.[11] From there, they can

---

[5] Paul R. Billings, *DNA Data Banks Would Taint Justice*, BOSTON GLOBE, Jan. 14, 1999, at A19 (op-ed), *available at* 1999 WL 6043488.

[6] *Id.*

[7] Dorothy Nelkin & Lori Andrews, *DNA Identification and Surveillance Creep*, 21 SOC. OF ILLNESS & HEALTH 689 (1999).

[8] E. Donald Shapiro & Michelle L. Weinberg, *DNA Data Banking: The Dangerous Erosion of Privacy*, 38 CLEV. ST. L. REV. 455 (1990); *cf.* Sheryl H. Love, *Allowing New Technology to Erode Constitutional Protections: A Fourth Amendment Challenge to Non-Consensual DNA Testing of Prisoners*, Jones v. Murray, 38 VILL. L. REV. 1617 (1993).

[9] The objections enumerated here are a pastiche collected from such articles as Philip L. Bereano, *The Impact of DNA-based Identification Systems on Civil Liberties*, *in* DNA ON TRIAL: GENETIC IDENTIFICATION AND CRIMINAL JUSTICE 119 (Paul R. Billings ed., 1992); Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767 (1999); Eric T. Juengst, *I-DNA-Fication, Personal Privacy, and Social Justice*, 75 CHICAGO-KENT L. REV. 61, 82 (1999); Jonathan Kimmelman, *The Promise and Perils of Criminal DNA Databanking*, 18 NATURE BIOTECHNOLOGY 695 (2000); Shapiro & Weinberg, *supra* note 8; Barry Sheck, *DNA Data Banking: A Cautionary Tale*, 54 AM. J. HUM. GENETICS 931 (1994); Michael J. Markett, Note, *Genetic Diaries: An Analysis of Privacy Protection in DNA Databanks*, 30 SUFFOLK U. L. REV. 185 (1996); Warren R. Webster, Jr., Note, *DNA Database Statutes and Privacy in the Information Age*, 10 HEALTH MATRIX 119 (2000). None of these commentators advances all of the objections, and a few come from concerns expressed by speakers or members of the audiences at conferences and symposia that I have attended.

[10] Some of these objections are considered more fully in D.H. Kaye, *Bioethics, Bench and Bar: Selected Arguments in* Landry v. Attorney General, 40 JURIMETRICS J. 193 (2000), and in Imwinkelried & Kaye, *supra* note 3. For discussions of constitutional objections to the practice, see D.H. Kaye, *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J.L. & PUB. POL'Y (forthcoming 2001) [hereinafter Kaye, *Constitutionality of Sampling*]; *see also* D.H. Kaye & Michael Smith, *DNA Databases for Law Enforcement: The Coverage Question and the Case for a Population-Wide Database*, *in* THE TECHNOLOGY OF JUSTICE: THE USE OF DNA IN THE CRIMINAL JUSTICE SYSTEM (David Lazer ed. forthcoming).

[11] Typically, the Local DNA Index System (LDIS), is installed at crime laboratories

be uploaded to a national database known as NDIS—the National DNA Index System—maintained by the FBI.[12] The compatible combination of local, state, and national databases is called CODIS (Combined DNA Index System). Police looking for the person who might have left blood, semen, or other biological trace evidence at crime scenes or on victims can search local, state, or national databases to learn whether a known offender might be the source of the crime-scene DNA.

In short, there are the *databases* that contain the data or records (the numerically coded, identifying genotypes), and the *databanks* or *repositories* that simply store the original samples taken from offenders.[13] If a match is found between a crime-scene DNA genotype and a genotype recorded in the database, further police work is required to establish a case against the suspect. If the full investigation suggests guilt and the case goes to trial, the prosecution should not rely on the database search to link the defendant to the crime. Rather, defendant's genotypes should come from the analysis of a new, confirmatory sample of the suspect's DNA.[14]

II. OBJECTIONS

The investigative practice described above may sound reasonable, but there is no shortage of objections that can and have been leveled against it.[15] The list of objections that follows is not exhaustive, and the analysis of them is not definitive. I do not pretend to resolve many issues, but I do hope to identify them and to indicate where the dialectic must begin.

---

operated by police departments or sheriff's offices. FBI, WHAT'S THE DIFFERENCE BETWEEN NDIS AND CODIS?, *available at* http://hope-dna.com/docs/difference_codis.htm (last visited Aug. 10, 2001).

[12] The FBI began implementing NDIS in October 1998, by combining the eight state DNA offender databanks in California, Florida, Illinois, Minnesota, North Carolina, Oregon, Utah and Virginia. *See* Nicholas Wade, *F.B.I. Set to Open Its DNA Database for Fighting Crime*, N.Y. TIMES, Oct. 12, 1998, at A1. In addition to the "convicted offender index," NDIS contains a "forensic index" of crime scene profiles permitting case-to-case matches, an "unidentified persons index," a "victims index," and a population database of anonymous DNA genotypes that can be used to estimate the probability that a DNA sample picked at random from the population would match a crime scene sample. Stephen J. Niezgoda & Barry Brown, *The FBI Laboratory's Combined DNA Index System Program*, *in* PROCEEDINGS FROM THE SIXTH INTERNATIONAL SYMPOSIUM ON HUMAN IDENTIFICATION 1995, at 149-52 (Promega Corp. ed., 1996).

[13] The phrase "DNA databanking" is somewhat imprecise. It could refer to the sample collections, the collections of records, or both. As used here, it denotes a repository of samples.

[14] If this sample matches the trace evidence DNA, then there is no need to introduce evidence of the database search, which would imply (possibly in violation of the rules of evidence) that the defendant has a criminal record.

[15] *See supra* note 9.

Objection: Criminal DNA databanking, which started with sex offenders, is expanding to encompass all offenders, including those who are no more likely than the ordinary citizen to leave DNA at a crime scene.

Response: This may (or may not) depict recent developments accurately, but it begs the question of whether the possible overbreadth is harmful.

Perhaps the most obvious question in the design of a compulsory databank or database is whose DNA should be taken. The trend is toward increased coverage of offenses. All states require sex offenders to give samples, and all but one[16] extend this requirement to most violent felonies.[17] Other statutes cast their net still more broadly, to reach all felons.[18] Many include certain misdemeanants as well.[19]

Nevertheless, the argument for restricting the databanks to felony sexual offenders is weak. Contrary to popular perceptions, sexual offenders are not more prone to repeat their offenses than are other offenders.[20] To be sure, some state databanks probably include groups who are no more likely than nonoffenders to leave DNA traces at future crimes. Ideally, these individuals would not be included in DNA databases, but some degree of overbreadth is not a fatal indictment of even the broadest systems. It is not always easy to tell exactly which groups of offenders are usefully incorporated into a database. We are dealing in probabilities both as to the recurrence of crime and the depositing of DNA. Moreover, where

---

[16] N.H. REV. STAT. ANN. § 632-A:21 (1999) The statute requires that:

> Before the release of any sexual offender after conviction, or of any juvenile sexual offender after finding of delinquency, whether on probation, conditional or unconditional release, completion of sentence, or release for any other reason, such person shall have a blood sample taken for DNA analysis to determine identification characteristics specific to the person.

Id.

[17] *E.g.*, CAL. PENAL CODE § 296 (West 1999) (listing criminal offenders subject to DNA sampling, including persons convicted of, or pleading guilty or no contest to, sex offenses, murder, voluntary manslaughter, spousal abuse, assault or battery, kidnapping, mayhem, and torture).

[18] *E.g.*, ALA. CODE § 36-18-24 (Supp. 2000) (extending DNA sampling to all "[p]ersons convicted after May 6, 1994 for a felony offense"). In such jurisdictions, activities such as sodomy, prostitution, and racketeering can result in inclusion in the state databank.

[19] *See* Kimmelman, *supra* note 9.

[20] *See* Katherine K. Baker, *Once a Rapist? Motivational Evidence and Relevancy in Rape Law*, 110 HARV. L. REV. 563, 578-80 (1997); Thomas J. Reed, *Reading Gaol Revisited: Admission of Uncharged Misconduct Evidence in Sex Offender Cases*, 21 AM. J. CRIM. L. 127, 149, 154-55 (1993); Paul R. Rice, *The Evidence Project: Proposed Revisions to the Federal Rules of Evidence*, 171 F.R.D. 330, 479 (1997).

plea bargaining is common, as it is in most metropolitan areas, the offense to which a defendant pleads does not always reflect the full nature of the actual conduct. Finally, unless some deprivation of an important interest would result from inclusion, apparent excesses in scope will not produce major injustices to individuals. Therefore, before concluding that databases should be constricted to a handful of offenses, we need to consider other objections that might reveal harms to individuals as a result of including their data in the system.

Objection: DNA identification is prone to error, and offender databanking is undesirable or unconstitutional because forensic DNA typing is not a mature enough technology to justify subjecting individuals to the risk of a false match.

Response: To err is human, but the technology is sound.

A false match could arise because either the databank sample or the trace evidence sample has been mischaracterized. Suppose that in creating the databank, Jones's DNA was switched with Smith's, and Jones is the true source of the evidence sample. The database search then will falsely incriminate Smith. But the database search should be the beginning, not the end of the investigation. Even in the unlikely event that the police have no other evidence against Smith, a confirmatory DNA test of a new sample taken from Smith will exclude him as a possible source of the evidence sample.

Furthermore, the state has every incentive to keep its database accurate. If mistyping of databank samples is common, perpetrators of crimes who are represented in the database will be missed. If samples are frequently mislabeled, subsequent exclusions should cause officials to grow frustrated with the system and to take corrective action. The resulting feedback makes DNA database searches more reliable than forensic techniques that typically involve unverified subjective assessments. For example, the polygrapher who reports on the basis of a "global assessment" that a suspect is lying no doubt believes that this "diagnosis" is accurate. He, after all, is trained in what he has been told is a powerful scientific procedure for resolving situations fraught with contradictions and ambiguity. Because it is the rare case in which any definitive evidence that would contradict the polygrapher will be generated, this kind of polygraphy easily becomes a self-fulfilling prophecy.

But even if the genotypes recorded in the database are all accurate, might not a false match arise from an error in the typing of the evidence sample? Ordinarily, it is extremely improbable that undetected defects in the equipment or reagents will distort the measurements so that they just

happen to match those of a single suspect. But when very large databases are searched, the chance of finding a match with someone is considerably larger. For instance, if the chance that errors would produce a match with any given genotype in the database is one in a million, but there are 10,000 genotypes, then the chance of a match with some previously unspecified genotype is approximately 10,000/1,000,000 = 1/100.

Quality control and quality assurance procedures should be employed to keep such errors to a minimum. The technology for discerning matches has made great strides since the earliest days of forensic work. Furthermore, in most cases, a portion of the evidence sample can be reserved for independent testing by another laboratory if the defendant doubts the accuracy of the match. For such reasons, the argument that DNA testing is so error-prone that offender databases will produce many false convictions, or even many false accusations, seems overdrawn.

Objection: Extracting DNA samples is a significant invasion of bodily integrity. It could be painful, physically harmful, or an interference with the general right to control one's own body.

Response: DNA sampling is minimally invasive.

A procedure for acquiring DNA that is painful or physically injurious would require substantial justification. Consider the well-known case, *Rochin v. California*.[21] Police broke into Rochin's room, saw him place two capsules in his mouth, struggled to extract them, took him to a hospital, and had a doctor force an emetic solution through a tube into his stomach. Rochin regurgitated two capsules of morphine. The Supreme Court held that this bodily invasion violated the right to due process of law. As Justice Frankfurter explained:

> This is conduct that shocks the conscience. Illegally breaking into the privacy of the petitioner, the struggle to open his mouth and remove what was there, the forcible extraction of his stomach contents . . . are methods too close to the rack and screw to admit of constitutional differentiation.[22]

However, the gulf between pumping the stomach in *Rochin* and extracting DNA for a database is huge. Only a small quantity of blood, other fluid, or buccal cells (on the inside of the cheek) is required, the sampling is minimally invasive, and the discomfort or danger associated with the procedure is slight. The intrusion is much closer to that involved

---

[21] 342 U.S. 165 (1952).

[22] *Id.* at 209-10.

in *Breithaupt v. Abram*.[23] In that case, police took a blood sample from an unconscious person who had been involved in a fatal accident and found a very high blood alcohol level. In concluding that this procedure was consonant with the "sense of justice" described in *Rochin*, the Supreme Court reasoned that "the interests of society in the scientific determination of intoxication, one of the great causes of the moral hazards of the road," outweighed "so slight an intrusion" of a person's body.[24]

In actuality, no one claims that DNA sampling is brutal. A more subtle version of the objection is that the extraction infringes the right to control access to one's body—regardless of whether the intrusion is physically painful or harmful. But this autonomy interest is very weak. Certainly, it is far removed from the interest protected in cases like *Griswold v. Connecticut*[25] and *Roe v. Wade*,[26] which established the right of individuals to make decisions about child-bearing for themselves—an aspect of liberty that could be overcome only by a compelling state interest. The state can override the more general privacy or liberty interest in controlling one's body when doing so bears a rational relationship to a legitimate state interest. Fingerprinting suspects in criminal investigations, vaccinating children, and ordering blood tests of parties (and non-parties) in paternity cases or in criminal investigations all interfere with the right to control one's body as one sees fit. They are not, for that reason, unethical or unconstitutional. As applied to gathering DNA, then, the interest in bodily autonomy is far too diffuse to preclude the practice of compiling convicted-offender DNA databases.

Objection: Because DNA is the "blueprint" or "future diary" of an organism, forensic genotyping reveals intensely personal information.

Response: The notion that we are the puppets of our DNA is naive, and, in any event, the genetic information used to match the trace evidence and the databank samples has no more meaning than a traditional fingerprint.

Although the modern Supreme Court has refused to elevate the general interest in the confidentiality of personal information to the level of a constitutional right,[27] in some circumstances, there is a socially important

---

[23] 352 U.S. 432 (1957).

[24] *Id.* at 439.

[25] 381 U.S. 479 (1965).

[26] 410 U.S. 113 (1973).

[27] *See* Whalen v. Roe, 429 U.S. 589 (1977); *see also* Edward J. Imwinkelried, *Can We Rely on the Alleged Constitutional Right to Informational Privacy to Secure Genetic Privacy*

interest in shielding information from public scrutiny. This interest is invaded when an eavesdropper listens to conversations even though the parties to the conversation are unaware of the eavesdropper, or when a peeping Tom looks into a window and keeps what he sees to himself. But these information-gathering acts are of concern only because a system that gives individuals a "private space" in which to be themselves is important. It has no application to DNA typing.

The aspect of informational privacy that does apply to genetic information lies in not having potentially stigmatizing genotypes exposed. However, the STR loci used in forensic identification are noncoding segments of DNA not known to be indicative of any functional characteristics or predictive of any diseases.[28] And, even if they were linked to some bodily or behavioral features, that would not necessarily implicate a meaningful privacy interest. One's blood type or eye color, for example, is genetically determined or influenced, but neither the genotypes nor the phenotypes are especially sensitive information. Analyzing DNA samples for forensic STRs produces a set of numbers that are useful for identification purposes and nothing else.[29]

Objection: DNA databanks contain personal information. Even if the loci used for identification are not subject to abuse, other loci associated with diseases or disease predispositions, or behavioral characteristics could be analyzed and used to stigmatize the donor.

Response: Either the samples should be purged, or there should be strong protection against unauthorized disclosure.

Determining individual identity by examining loci associated with diseases would be inefficient and would not offer any significant advantage over the loci now used in offender databanking.[30] Consequently, there is little reason to believe that the law enforcement community will move in this direction. If the prospect were more real, it might be appropriate to

---

in the Courtroom?, 31 SETON HALL L. REV. 926 (2001).

[28] *See, e.g.*, JOHN M. BUTLER, FORENSIC DNA TYPING 245 (2001).

[29] *Id.* However, these loci could be used to infer relationships such as parentage if samples from the potentially related individuals were typed.

[30] Genes associated with debilitating or other diseases that affect reproductive success of an individual or close kin are subject to natural selection. Even a small reduction in reproductive fitness will disappear over many generations. The result is that the forensic loci, which do not experience selection pressure, tend to have more alleles than the coding regions. The increased variability gives these loci greater power to differentiate among individuals. *See* NATIONAL RESEARCH COUNCIL, COMMITTEE ON DNA FORENSIC SCIENCE: AN UPDATE, THE EVALUATION OF FORENSIC DNA EVIDENCE 117 (1996).

specify that no known disease or behavior-related loci be used in law enforcement databases.

The fear that health insurers or employers will use genetic information to screen applicants for policies or jobs is widespread, despite the lack of evidence of much genetic "discrimination" so far.[31] Indeed, this fear has prompted a spate of legislation forbidding such actions.[32] In addition, genetic privacy legislation enacted in many states forbids the collection or dissemination of genetic information about an individual without explicit consent.[33] Although the latter legislation generally does not apply to law enforcement databanks or databases, the statutes establishing the databases often proscribe and penalize unauthorized disclosures of any kind.[34] The notion that many insurers and employers will approach the police laboratories for samples of DNA when they are considering insuring or hiring former offenders seems far-fetched.[35]

The strongest possible protection against unauthorized disclosure of samples would be the destruction of the samples after they are genotyped.[36] Now that we are in the third generation of typing methods,[37] the need to retain samples in the event that new loci will be adopted is abating.[38] The current policy of retaining the samples year after year should be re-examined.

---

[31] There are relatively few documented instances of insurers or employers using surreptitiously obtained DNA samples. *See* D.H. Kaye, *Respecting Genetic Privacy: The ASU-SB Conference on Law, Science, Technology: A Foreword*, 40 JURIMETRICS J. 1, 6 n.26 (1999). There are no known instances of law enforcement authorities sharing DNA samples with outside employers or insurers.

[32] *See, e.g.*, William F. Mulholland & Ami S. Jaeger, Comment, *Genetic Privacy and Discrimination: A Survey of State Legislation*, 39 JURIMETRICS J. 317 (1999); Helen R. Davis & Janis V. Mitrius, Note, *Recent Legislation on Genetics and Insurance*, 37 JURIMETRICS J. 69 (1996).

[33] *See* sources cited *supra* note 29.

[34] *See, e.g.*, DEL. CODE ANN. tit. 29, § 4713(l) (1997) ("Any person who disseminates, receives or otherwise uses or attempts to use information in the database, knowing that such dissemination, receipt or use is for a purpose other than authorized by law, shall be guilty of a Class A misdemeanor.").

[35] When the government is itself the employer, the concern is somewhat more realistic. *See* Sally Lehrman, *Medical Tests Cost Lawrence Berkeley $2.2 Million*, 405 NATURE 110 (2000).

[36] *See* NATIONAL RESEARCH COUNCIL COMMITTEE ON DNA TECHNOLOGY IN FORENSIC SCIENCE, DNA TECHNOLOGY IN FORENSIC SCIENCE 122 (1992) ("As databanks become established and technology stabilizes somewhat, samples should be destroyed promptly after typing.").

[37] The first generation involved RFLP tests for VNTR loci. The second involved PCR-based tests for various coding loci. The third involves PCR-based tests of noncoding STR loci. *See* 1 MCCORMICK ON EVIDENCE § 205 (John Strong ed., 5th ed. 1999).

[38] Database administrators also suggest that sample retention is valuable for quality control purposes. Retyping of the original sample may be required before a hit is declared and police are notified.

Objection: Offender databases and databanks should be used solely for criminal justice purposes. Some states explicitly allow the information in the database to be used, pursuant to a court order, in proceedings establishing parent-child relationships. Many laws allow DNA database information to be released for "law enforcement purposes" or by court order—provisions that could be brought to bear in civil proceedings.

Response: Some additional uses pose no risks or harms.

If the sampling is justified by criminal law enforcement needs and a civil party who happens to have contributed to the databank could be ordered by a court to submit to DNA sampling for civil discovery anyway, it is hard to understand what interest is invaded by using the previously submitted sample.

Objection: DNA databanking invades the privacy of innocent relatives. In rare circumstances, database searches might implicate an offender's relative rather than the previously convicted offender himself. For instance, if the closest thing to a complete match is a match at eleven out of thirteen loci, everyone in the database is excluded, but it is very likely that the trace evidence DNA comes from someone closely related to the individual who matches at the eleven loci rather than from an unrelated person.

Response: It is true that the relative might not have been suspected but for the database search, but the search does not violate any cognizable privacy right of the relative.

Relatives have no right to be free from exposure to police investigation. Suppose that a rape victim studying mugshots reported that a picture on file looked exactly like the rapist, except that the rapist had orange hair, and the man in the photograph has brown hair. Suppose further that the police establish that the convicted offender whose mugshot is on file had brown hair at the time of the rape. However, they also learn that the convicted offender has an identical twin who dyed his hair orange. Could the twin object to his becoming a target of the investigation because *he* did nothing that would justify the police having his brother's picture in their files? As with the mugshot, if the DNA sample was properly obtained, there would be no reason to prohibit its use as an investigatory lead to a relative.[39]

---

[39] *See* Imwinkelried & Kaye, *supra* note 3.

Objection: Using samples from offender databanks for population genetics research or behavioral genetics research violates the Nuremberg Code. The Nuremberg Code makes informed consent for medical research essential, and databanking laws should ensure that the DNA samples be used solely for casework (and perhaps intimately related research such as studies of STR frequencies).

Response: It might (or might not) be desirable to withhold samples from genetics researchers, but not because of the Nuremberg Code.

The Nuremberg Code is a list of ten "basic principles" of ethical "medical experiments on human beings" promulgated by the United States military tribunal that found fifteen of twenty-three Nazi doctors guilty of participating in "plans and enterprises involving medical experiments without the subjects' consent . . . in the course of which experiments the defendants committed murders, brutalities, cruelties, tortures, atrocities, and other inhuman acts."[40] The first principle in the Code is that "[t]he voluntary consent of the human subject is absolutely essential."[41]

But is the use of a banked sample for research into violence or other behaviors a "medical experiment on human beings?" Certainly, this is not what the tribunal had in mind when it formulated the Code. That court was concerned with doctors who, among other things, injected concentration camp inmates with yellow fever, smallpox, typhus, cholera, diphtheria, and spotted fever to test vaccines, who immersed inmates in freezing water until they died to test methods for treating hypothermia, who transplanted sections of bones from one inmate to another, and who fed inmates poisons or shot them with poisoned bullets. The Code itself speaks in terms that presume that a specific human being is the subject of an investigation into the treatment of a disease or comparable condition. Consistent with this understanding, contemporary medical researchers have not found it clearly unethical to use banked tissue samples without obtaining explicit consent from the donors.[42]

---

[40] United States v. Brandt (The Medical Cases), 2 Trials of War Criminals Before the Nuremberg Military Tribunals Under Control Council Law No. 10 (1949).

[41] The Nuremberg Code, *available at* http://www.ushmm.org/research/doctors/Nuremberg_Code.htm (last visited Aug. 20, 2001).

[42] *See* Henry T. Greely, *Breaking the Stalemate: A Prospective Regulatory Framework for Unforeseen Research Uses of Human Tissue Samples and Health Information*, 34 WAKE FOREST L. REV. 737 (1999); Kaye, *Constitutionality of Sampling*, *supra* note 10; David Korn, *Genetic Privacy, Medical Information Privacy, and the Use of Human Tissue Specimens in Research*, *in* GENETIC TESTING AND THE USE OF INFORMATION 16 (Clarisa Long ed., 1999).

Of course, recognizing that the invocation of the Nuremberg precedent is frightfully wide of the mark does not mean that research with banked DNA samples should be permitted. Indeed, many, if not most, statutes either do not authorize or explicitly foreclose the release of samples for medical research.[43] However, the issue cannot be decided by a talismanic incantation of the necessity for informed consent. Indeed, in contrast to the tissue banks established in the context of health care or research, offender DNA samples were not provided voluntarily in the first place, but were compelled in the public interest.

Of course, if some actual harm might flow from the research, it would be inappropriate to disseminate the samples. There are two related possibilities. First, if the research uncovered a set of genes affecting the propensity for rape or other criminal behavior, the researchers would know whether a person whose DNA was used in the study had the alleles associated with such behavior. Second, the researchers might analyze other, previously studied genes that an individual would not have wished to have revealed to anyone. One way to avoid these privacy problems would be to anonymize the samples before they reach the researchers.[44]

Finally, some scientists and ethicists oppose all research "designed to identify genes associated with criminal behavior" on the grounds that "such research has no scientific merit" and "could be used as a new biological justification to bolster racist and ethnic prejudice."[45] However, the claim that all behavioral genetics research relevant to crime is unscientific seems more dogmatic than scientific. If at least some research has scientific merit, one must confront the question whether the state should discourage research because the knowledge it produces might affect the opinions of its citizens.

CONCLUSION

DNA databases for law enforcement are growing rapidly. Most of the criticisms surfacing in the legal and bioethical literature reflect important concerns, but some of the discussions manifest excessive fears. The databases must be designed and administered in ways that fully respect the rights and interests of all individuals. To contribute to this result, studies of

---

[43] *See, e.g.*, Landry v. Attorney General, 709 N.E.2d 1085, 1096 (Mass. 1999).

[44] It is sometimes suggested that there is no such thing as anonymity with DNA samples. This claim is fatuous in the context of identification databanks. To determine the identity of an anonymous DNA sample, one would need another DNA database of named individuals. That is what the law enforcement database is for, and it is hard to imagine that the researchers would have comparable databases at their disposal.

[45] Nachama L. Wilker et al., *DNA Data Banking and the Public Interest*, in DNA ON TRIAL: GENETIC INFORMATION AND CRIMINAL JUSTICE 141, 147 (Paul R. Billings ed., 1992).

the bioethics of DNA databanks and databases must rest on accurate and realistic assessments of the nature and dangers of the technology as well as careful analyses of the pertinent individual rights and responsibilities. Undertaking these evaluations remains a challenge for lawyers, ethicists, and all citizens concerned with the impact of forensic technology on individual rights.