Am. J. Hum. Genet. 54:941-958, 1994

A Review of State Legislation on DNA Forensic Data Banking

Jean E. McEwen*,† and Philip R. Reilly*

*Eunice Kennedy Shriver Center for Mental Retardation, Division of Social Science, Ethics, and Law, Waltham, MA; and †Boston College Law School, Newton, MA

Summary

Recent advances in DNA identification technology are making their way into the criminal law. States across the country are enacting legislation to create repositories for the storage both of DNA samples collected from convicted offenders and of the DNA profiles derived from them. These data banks will be used to assist in the resolution of future crimes. This study surveys existing state statutes, pending legislation, and administrative regulations that govern these DNA forensic data banks. We critically analyzed these laws with respect to their treatment of the collection, storage, analysis, retrieval, and use of DNA and DNA data. We found much variation among data-banking laws and conclude that, while DNA forensic data banking carries tremendous potential for law enforcement, many states, in their rush to create data banks, have paid little attention to issues of quality control, quality assurance, and privacy. In addition, the sweep of some laws is unnecessarily broad. Legislative modifications are needed in many states to better safeguard civil liberties and individual privacy.

Introduction

The United States in the past 5 years has witnessed an explosion in DNA technology. In the forensics context, the rise of this technology has been accompanied by a heated debate and a rapid proliferation of commentary concerning the reliability of DNA analysis for identification testing (Roberts 1991; Anderson 1992; National Academy of Sciences 1992). However, this discussion has focused almost exclusively on the standards for the admissibility of DNA evidence in court. Underconsidered in the debate have been the distinct issues raised by the rapid and continuing emergence of state statutes that authorize crime laboratories to create repositories for the long-term storage of DNA (DNA banks) or of profiles derived from DNA (DNA data banks).

The data-banking laws that are the subject of this article generally require certain criminal offenders to submit a blood sample at the time of sentencing or before release from prison. Crime laboratories will then extract DNA from these samples and, using what is becoming a nationally uniform set of probes and enzymes, analyze them for identification (National Academy of Sciences 1992). The resulting profiles, arguably unique to each individual (with the exception of identical twins) will then be stored on computer. Under the evolving system, law-enforcement officials confronted with an anonymous evidence sample (such as semen from a rape victim) will eventually be able to access a network of data banks across the country, in search of a match with the sample profile—much the same as is now done with conventional fingerprints (United States Congress 1990). The Federal Bureau of Investigation (FBI) has taken the lead in transferring DNA identification technology to state and local crime laboratories and will facilitate information transfer between data banks, through a System called "CODIS" (Combined DNA Identification system) (Technical Working Group on DNA Analysis Methods 1989). CODIS will involve a centralized index that references the sources of all DNA profiles, with supporting records maintained at the state level.

The proposed national network of DNA data banks will, when fully operational, facilitate the apprehension of suspects who in many cases might otherwise go undetected. DNA forensic data banks hold particular promise for rape cases, where the rate of recidivism—

Received October 7, 1993; accepted for publication February 9, 1994.

Address for correspondence and reprints: Jean E. McEwen, J.D., Shriver Center for Mental Retardation, Division of Social Science, Ethics, and Law, 200 Trapelo Road, Waltham, MA 02254.

0002-9297/94/5406-0003$02.00

the likelihood that an offender will repeat his crime—is extraordinarily high, and for other violent crimes (United States Department of Justice, Bureau of Justice Statistics 1989).

The DNA Identification Act of 1993 (H.R. 829, S. 497, 103d Cong., 1st sess.), pending in Congress, which, if enacted will make data banks in individual states eligible for federal grants in exchange for adherence to certain quality assurance and proficiency-testing standards, will greatly expand states' data-banking capabilities (DNA Identification Act of 1993, H.R. 829, S. 497, 103d Cong., 1st sess.). The FBI has developed legislative guidelines for drafting state DNA forensic data-banking laws that loosely track the provisions of this federal legislation (United States Department of Justice, Federal Bureau of Investigation 1991). However, the ability of the FBI to set adequate regulatory standards regarding DNA data banking or DNA analysis generally—either for itself or for the state and local crime laboratories that it oversees—has been called into serious question (National Academy of Sciences 1992). Indeed, many existing state laws seem to have been drafted with little consideration of their possible effects and with few protections against security abuses.

Balancing the benefits and risks inherent in DNA forensic data banking requires an understanding of the legal framework in which data banks operate and of how the crime laboratories that develop them conduct their activities. In this article, we survey and analyze the laws that govern data-banking activities. A second article, now in preparation, will report the results of an empirical survey of crime-laboratory personnel, regarding day-to-day data-bank operations (J. E. McEwen, unpublished data).

Material and Methods

Using a combination of the computer-assisted legal research methods LEXIS and WESTLAW and traditional manual legal research methods, we identified (1) all state statutes enacted as of December 31, 1993, that create DNA forensic data banks; (2) all pending state legislation on DNA forensic data banking (excluding appropriations bills) introduced during the 1993 legislative sessions; and (3) all administrative regulations issued under existing data-banking laws. Existing statutes were located using statutory databases available on LEXIS and WESTLAW and the annotated codes of each state. Citations to pending bills were located using bill-tracking databases on LEXIS and WESTLAW; the full text of each bill was obtained for analysis, from the legislative reporting service in each relevant state. Regulations were located in the official administrative codes of those states that have relevant statutes.

We critically analyzed the content of the full text of all materials, with respect to procedures for the collection, storage, analysis, retrieval, and use of samples and related data. We also tracked the history of each statute, in an effort to identify common legislative trends. In addition, we examined relevant case law and federal guidelines.

Results

As of December 31, 1993, 19 states had enacted laws that authorize or (except in the case of one state) mandate the establishment of DNA forensic data banks (see table 1). In addition, during the 1993 legislative sessions, legislation on DNA forensic data banking was introduced in 10 states (in some cases, with more than one bill per state). The proposed bills in three states would amend existing laws (see table 2), while the bills in the remaining seven states would create new data banks (see table 3). Thus, by next year, approximately half of all states may have DNA forensic data-banking laws.

In some states with data-banking laws, the legislatures have not yet appropriated funds sufficient to implement the legislation. Thus, the data banks authorized in many states have not yet become operational—because they either do not yet have the resources to collect samples or lack the DNA laboratories or trained personnel needed to analyze them. Louisiana, which previously had a data-banking law, repealed its statute in 1993 because of its legislature's failure to appropriate funds for the law's implementation.

Responsible Agency and Authorized Purposes

Overall responsibility for the operation of the DNA forensic data banks in most states resides in the forensics unit of either the state bureau of investigation or the department of public safety (or their state-specific equivalents). In several states the responsible agencies have issued administrative regulations pursuant to the enabling legislation, to govern the day-to-day operation of the data bank (see table 4).

In some states the sentencing court or corrections department assumes responsibility for collecting samples, while the designated investigative or law-enforce-

Table 1

State Statutes, Enacted as of December 31, 1993, That Authorize or Mandate the Establishment of DNA Forensic Data Banks

State	Year Enacted	Citation
Arizona	1989	Ariz. Rev. Stat. Ann. § 3-281
California	1983	Cal. Penal Code § 290.2 (West)
Colorado	1988	Colo. Rev. Stat. § 17-2-201
Florida	1989	Fla. Stat. Ann. § 943.325 (West)
Georgia	1992	Ga. Code Ann. § 24-4-60, et seq.
Hawaii	1991	Haw. Rev. Stat. § 706-603
Illinois	1990	Ill. Ann. Stat. ch. 38, par. 1005-4-3 (Smith-Hurd)
Iowa	1989	Iowa Code Ann. § 13.10 (West)
Kansas	1991	Kan. Stat. Ann. § 21-2511
Kentucky	1992	Ky. Rev. Stat. Ann. §§ 17.170, 17.175 (Michie/Bobbs-Merrill)
Michigan	1990	Mich. Stat. Ann. §§ 4.484(1), et seq., 28.788(13), 28.2303(5) (Callaghan)
Minnesota	1989	Minn. Stat. Ann. §§ 299C.155, 609.3461 (West)
Missouri	1991	Mo. Ann. Stat. § 650.050 (Vernon)
Nevada	1989	Nev. Rev. Stat. Ann. §§ 176.111, 179A.075 (Michie)
Oregon[a]	1991	Or. Rev. Stat. §§ 181.085, 137.076, 161.325
South Dakota	1990	S.D. Codified Laws Ann. §§ 23-5-14, et seq.
Tennessee	1991	Tenn. Code Ann. §§ 38-6-113, 40-35-321
Virginia	1990	Va. Code Ann. § 19.2-310.2, et seq. (Michie)
Washington	1989	Wash. Rev. Code Ann. §§ 43.43.752, et seq. (West)

NOTE.—Louisiana's data-banking statute was repealed in 1993. La. Rev. Stat. Ann. §§ 15:535, 15:536, 15:578, repealed, 1993 La. H.B. 883 (6/21/93).

[a] Oregon's statute authorizes but does not mandate the establishment of a DNA data bank; all other statutes require states to set up data banks.

ment agency handles the storage and analysis of samples and maintains the data bank. In South Dakota, where data-bank samples can be taken from persons who have merely been arrested and not yet convicted, the attorney general, in cooperation with various law-enforcement officials, is responsible for collection; samples are then submitted to the state's division of criminal investigation, for analysis. In Washington State, the police maintain the data bank in consultation with the state university school of medicine.

Table 2

State Legislation, Introduced during 1993 Legislative Sessions, to Amend Existing DNA Forensic Data-banking Laws

State	Date Introduced	Bill
Arizona	February 2, 1993	Senate bill 1217
California	January 25, 1993	Assembly bill 201
	February 3, 1993	Assembly bill 304
Minnesota	March 18, 1993	Senate bill 1024

The data banks exist for the express purpose of assisting law enforcement. However, some of the statutes do not precisely define the term "law enforcement," leaving it unclear whether a data bank can be accessed *only* in furtherance of an official investigation of a specified criminal offense or whether it can be used in other situations. Currently, only Kentucky expressly permits use of its data bank for assistance in locating missing persons or in identifying unknown human remains.

Most statutes provide no explicit authorization for the retention in data banks of DNA data derived from evidence either left at crime scenes or obtained from victims. However, California, Minnesota, and Tennes-

Table 3

State Legislation, Introduced during 1993 Legislative Sessions, to Authorize the Establishment of New DNA Forensic Data Banks

State	Date Introduced	Bill
Delaware	May 11, 1993	House bill 198
	June 23, 1993	House bill 318
Massachusetts	January 6, 1993	Senate bill 685
New York	May 14, 1993	Senate bill 4944 (governor's program bill)
	February 2, 1993	Assembly bill 2566
	March 22, 1993	Senate bill 3797
	June 3, 1993	Assembly bill 8274
North Carolina	April 19, 1993	House bill 1050
Texas	February 19, 1993	House bill 988
	March 5, 1993	House bill 1545
	March 11, 1993	House bill 2376
	March 11, 1993	House bill 2381
Vermont	February 15, 1993	Senate bill 190
Wisconsin	June 17, 1993	Assembly bill 589

Table 4

Administrative Regulations, Issued as of December 31, 1993, Governing the Operation of DNA Forensic Data Banks

State	Year Issued	Citation
Florida	1990	Fla. Admin. Code Ann. r. 11D-6.001, et seq.
Iowa	1991	Iowa Admin. Code r. 61-8.1 (13), et seq.
Oregon	1991	Or. Admin. R. 257-60-005, et seq.
South Dakota	1990	S.D. Admin. R. 2:04:01:01, et seq.
Washington	1991	Wash. Admin. Code §§ 446-75-010, et seq.

see do specifically contemplate the inclusion of such data, and new legislation pending in Texas contains a similar provision. By contrast, in Washington State, pursuant to an administrative regulation, DNA identifications made in the context of a criminal investigation *cannot* be entered into any permanent or temporary data bank; rather, they must be returned to the agency that requested them.

To date, only the California, Georgia, Kentucky, Oregon, and Virginia statutes *explicitly* contemplate using their offender samples (anonymously) for creating separate population-statistics data banks (reference bases for calculating allele frequencies). However, most data banks presumably can be adapted to this use, even without explicit statutory authorization, so long as the offender's identity cannot be determined. Legislation now under consideration in Vermont would authorize the creation of a separate statistical DNA data bank compiled from a reference population of persons whose identity is unknown. The Vermont bill does not specify whether the persons to be included in this data bank would be criminal offenders, nonoffenders, or both.

New bills pending in New York, North Carolina, and Texas will, if enacted, authorize the establishment of DNA data banks in each of those states, for a wide range of purposes. In addition to allowing the use of anonymous DNA samples and profiles to create reference data banks to designate allele frequencies, they would permit access to samples for research, developing DNA testing protocols, and quality-control purposes. These bills, as well as the proposed Delaware bill, would also allow the data banks to be used to assist in identifying human remains and in recovering missing persons.

Categories of Offenders Included

Statutes that authorize the extraction of DNA samples from convicted offenders for data banking vary widely in the range of offenses that they encompass (see table 5). However, without exception, felony sex offenses (sex offenses for which the punishment is generally more than 1-year imprisonment) are covered. These crimes typically include rape and various degrees of criminal sexual assault; habitual sex offenders also fall under this category. However, violent acts are not always necessary for a crime to be elevated to the level of a felony. Indeed, some states' data-banking laws include sex offenses that, while technically felonies, do not characteristically involve violence and are not the types of crimes where biological evidence tends to be

Table 5

Categories of Crimes Covered by Existing DNA Forensic Data-banking Laws

State	Sex-related Felonies	Other Felonies	Sex-related Misdemeanors
Arizona	X	X	
California	X	X	X[a]
Colorado	X		X
Florida	X		X
Georgia	X		
Hawaii	X	X	X
Illinois	X		X
Iowa	X	X	
Kansas	X	X	X
Kentucky	X		X
Michigan	X		X
Minnesota	X		
Missouri	X	X	
Nevada	X		
Oregon	X	X	X
South Dakota	X		X
Tennessee	X		
Virginia	X	X	
Washington	X	X	

[a] Also covers some non-sex-related misdemeanors.

left at the scene. For example, Oregon's statute applies to persons convicted of promoting or compelling prostitution. The former Louisiana statute (now repealed) included engaging in or abetting bigamy—a crime classified as a felony under the state's criminal code.

Only four states' laws limit their reach to collecting samples *exclusively* from felony sex offenders. Eleven states' statutes also cover one or more sex offenses that can be treated as misdemeanors (punishable by fine, probation, or a jail term of <1 year). These misdemeanors typically include lewd and lascivious conduct (e.g., "peeping toms"), lesser degrees of sexual assault, and indecent exposure. Some of these statutes include sex-related misdemeanors that involve no violence and that do not tend to be associated with biological evidence. For example, California's data-banking requirement extends to the misdemeanor of loitering near public toilets, and South Dakota includes the possession of child pornography.

Seven statutes, in addition to covering felony sex offenses (and, in some cases, sex-related misdemeanors), cover other types of felonies. For example, Florida's law, which originally included only specified sex offenses, was amended in 1993 and now also includes murder and attempted murder. Typically, the covered non–sex-related felonies do involve such serious, violent crimes. Several states, however, list a wide range of felonies, some of which are not generally associated with biological evidence and/or necessarily with high rates of recidivism. For example, Missouri's data-banking requirement extends to persons convicted of elder abuse, interfering with a court officer, and interference with child custody. California's law applies to persons convicted of assault with a stun gun on a school employee, and Washington's law applies to vehicular homicide caused by drunk or reckless driving. Virginia's law covers *all* convicted felons.

California, which currently has one of the broadest DNA data-banking laws, requires the collection of samples for DNA analysis even from persons convicted of certain non–sex-related misdemeanors. Covered offenses there include certain types of assault and battery on custodial officers, transportation personnel, or jurors; contributing to the delinquency of a minor; and inducing disobedience to a court order. This represents a considerable expansion of California's original data-banking law, which, when enacted in 1983 as the nation's first such law, required only adult registered sex offenders to submit blood and saliva samples for serological testing.

Much of the newer legislation that has not yet been enacted but is now under consideration would apply to an even broader range of crimes. The bill under consideration in Massachusetts would apply to the misdemeanor of using "profane, obscene, or impure language or slanderous statements [in] a sporting event" (Mass. Senate bill 685, 1993)! The major bill pending in New York would apply to the issuance of "abortional articles" (New York Senate bill 4944, 1993) The proposed North Carolina bill would encompass those convicted of any of 22 crimes, ranging from malicious castration or maiming and the malicious throwing of corrosive acid or alkali to the burning of a mobile or recreational trailer home. Vermont's pending bill would require samples from persons convicted of "violent crimes," but that term is broadly defined to include such offenses as stalking, lewd and lascivious conduct, and drunk driving that results in death or serious injury, as well as a variety of other motor-vehicle offenses. In Texas, one of several bills under consideration would apply to persons convicted of aiding suicide; language in several of the other bills would authorize taking samples from *any* prison inmate.

On the other hand, the new bills pending in Delaware and Wisconsin would apply *only* to sex offenders. The Wisconsin bill also differentiates between degrees of sex offenses; it provides for automatically taking samples from those convicted of the most serious offenses but gives the sentencing court discretion to decide—on the basis of such circumstances as the victim's age, whether force was used or threatened, and the defendant's criminal history record—whether to require samples from less serious offenders.

Treatment of Juvenile Offenders and Transferees—and Plea Bargains

The data-banking laws in a number of states expressly apply to youthful offenders or minors adjudicated as delinquent—at least in connection with certain specified offenses (see table 6). Although one state specifically excludes juveniles from its law, five other states' laws, as well as the new bills pending in Massachusetts and Wisconsin, specifically *include* them. The data-banking requirement would also presumably apply in other states where juvenile offenders can be tried and convicted as adults. California's statute did not encompass juveniles when it was first enacted, but in 1985 it was amended to include them. Likewise, Kansas first added a reference to juvenile offenders to its law in 1992.

Table 6

Coverage of Juvenile Offenders under Existing DNA Forensic Data-banking Laws

State	Covered	Excluded	Unspecified
Arizona			X
California	X		
Colorado			X
Florida			X
Georgia			X
Hawaii			X
Illinois			X
Iowa			X
Kansas	X		
Kentucky			X
Michigan			X
Minnesota	X		
Missouri			X
Nevada		X	
Oregon	X		
South Dakota			X
Tennessee	X		
Virginia			X
Washington			X

Most statutes do not directly address the treatment of persons who were convicted of similar offenses under the laws of other states and who later are transferred into the correctional system of the state in question. In Iowa, however, an administrative regulation requires such offenders to provide a sample. Likewise, a proposed amendment to Minnesota's data-banking law would make acceptance of a prisoner transferred from another state for reasons of prison overcrowding conditional on the offender's providing a sample for the Minnesota data bank.

Most states' statutes require a *conviction* of a *covered* offense before samples can be taken for the data bank, but certain exceptions exist. As mentioned, South Dakota law authorizes the collection of samples from persons who have merely been arrested. In addition, the bill recently introduced in Massachusetts will, if enacted, require samples from persons whose cases are merely continued without a finding or who plead to a lesser offense and admit to sufficient facts to warrant a guilty finding. Likewise, in Minnesota, a bill under consideration would amend the data-banking statute to encompass those merely charged with a covered offense but ultimately convicted of another offense arising out of the same set of circumstances. The proposed Wisconsin bill would apply to those found, by reason of a mental disease or defect, not guilty of a covered offense.

Effective Date and Timing of Sample Collection

In most states, the requirement that offenders provide a sample for the data bank extends not only to those who are convicted after the statute's effective date, but also to those who were already incarcerated —by requiring them to supply a sample at some specified point before release (see table 7). However, some statutes, by their terms, apply only prospectively—to persons convicted after the statute's effective date. Other statutes are silent on whether the requirement applies retroactively, and presumably, in those states, the law *could* be so applied, subject to the possibility of future court challenge. The new bill pending in Massachusetts would apply to persons previously convicted of a covered offense who have already been either placed on probation or recently released through furlough, parole, prerelease, or work release.

The *timing* of sample collection depends on whether the sample is being taken from a new offender or from one who is already incarcerated. For new offenders, the statutes variously require collection "upon convic-

Table 7

Retroactive or Prospective Application of Existing DNA Forensic Data-banking Laws

State	Retroactive	Prospective	Unspecified
Arizona		X	
California	X		
Colorado		X	
Florida		X	
Georgia		X	
Hawaii			X
Illinois	X		
Iowa	X		
Kansas	X		
Kentucky	X[a]	X[a]	
Michigan	X		
Minnesota	X		
Missouri			X
Nevada			X
Oregon			X
South Dakota	X		
Tennessee		X	
Virginia	X		
Washington		X	

[a] "May" collect from already incarcerated offenders and "shall" collect from new offenders.

tion," within a specified number of days after conviction or sentencing, within a "reasonable time" after sentencing, or immediately on arrival at the correctional facility. In South Dakota, where samples can be taken from mere arrestees, samples are taken immediately on the arrest.

A bill is pending to amend California's statute to prohibit taking a sample until all appeal rights have been exhausted or waived or until the time for an appeal has lapsed. By contrast, the Massachusetts bill has a provision stating that collection cannot be postponed while a conviction or sentence is under appeal.

In those states where the statutes apply to convicted offenders who are already incarcerated, some laws provide for the taking of samples just before final discharge (e.g., as a condition of release on parole). Others merely require collection at an unspecified time during the term of confinement.

California and some other states require "habitual" sex offenders to submit a sample as part of a more general registration requirement, under which such offenders, in accordance with other laws, are required to "report in" to authorities on a periodic basis. The habitual sex-offender DNA data-banking laws, because they are often incorporated into existing registration requirements, contain special provisions for the timing of sample collection and also tend to apply retroactively.

Nature of Samples Collected and Specific Collection Procedures

Most of the enabling statutes specify the type of tissue samples that can or must be collected for the data bank (see table 8). The vast majority refer specifically to the extraction of blood, but eight states also authorize the collection of saliva. In three other states, the statutes refer only to the taking of "biological or physical specimens."

Few statutes dictate the location for sample collection, presumably leaving this detail to the discretion of the responsible agency. Where samples are being taken from already incarcerated offenders, collection generally takes place inside the prison. However, samples taken from new offenders—particularly those who are not being sentenced to a term of confinement—are usually taken at a different location. Hawaii provides the greatest leeway, authorizing collection at "any available clinic or hospital, intake service center, community correctional center, or state or county health department facility" (Haw. Rev. Stat. §706-603).

A few states exempt offenders from providing an additional sample for the data bank if an adequate sample is already on file (e.g., in connection with the investigation of the underlying case). Oregon also provides an exemption when the extraction of blood would present an unreasonable risk to the health of the offender. On the other hand, the Illinois statute, as amended in 1992, expressly requires the offender's cooperation in sample collection and makes punishable, as contempt of court, any deliberate act intended to impede it. The new bill under consideration in Wisconsin would mandate the imposition of fines ≤$10,000 and/or imprisonment of ≤9 mo for offenders who intentionally fail to comply with the collection requirement.

Several statutes explicitly state that sample collection must be done in a "medically approved manner," and in most states samples can only be taken by or under the direction of certain specified professionals, ranging from physicians and registered nurses to laboratory technicians and phlebotomists. However, a few states merely require collection by a "qualified person," and some statutes are silent on the qualifications of the collection agent.

A number of statutes expressly immunize from legal liability the person or agency collecting the sample, so long as the sample is withdrawn with "ordinary care"

Table 8

Nature of Samples Collected under Existing DNA Forensic Data-banking Laws

State	Blood	Saliva	Unspecified
Arizona	X		
California	X[a]	X	
Colorado	X	X	
Florida	X[a]		
Georgia	X		
Hawaii	X[a]	X	
Illinois	X	X	
Iowa	X		
Kansas	X	X	
Kentucky	X		
Michigan	X	X	
Minnesota			X
Missouri	X		
Nevada	X	X	
Oregon	X		
South Dakota	X	X	
Tennessee			X
Virginia	X		
Washington	X		

[a] Two samples required.

Table 9

Safeguards against Sample Mix-ups and Tampering under Existing DNA Forensic Data-banking Laws

State	Yes	No
Arizona		X
California		X
Colorado		X
Florida	X	
Georgia	X	
Hawaii		X
Illinois		X
Iowa		X
Kansas		X
Kentucky		X
Michigan		X
Minnesota		X
Missouri		X
Nevada		X
Oregon	X	
South Dakota	X	
Tennessee		X
Virginia	X	
Washington		X

and in accordance with "generally recognized medical procedures." However, some statutes recognize an exception to immunity when blood is withdrawn negligently.

Safeguards against Sample Mix-ups and Tampering

In many states, pursuant to either statute or regulation, the responsible agency provides all the materials needed for collection, including specimen vials, mailing tubes, labels, and instructions. Beyond this, however, few statutes contain specific provisions designed to prevent sample mix-ups or tampering. Florida, under regulations issued by the responsible agency, is the only state that expressly requires offenders to be positively identified before samples can be taken. No statutes require a photograph of the offender to accompany the sample.

The Kentucky statute, as well as the new bill pending in Delaware and one of several bills pending in Texas, classifies tampering with samples as a felony. However, only two states' statutes (and administrative regulations in three others) contain detailed provisions to ensure against this possibility (see table 9). Georgia and Virginia, for example, require all collection tubes to be labeled with the offender's name, social security number, date of birth, race, and gender, as well as with both the name of the person collecting the sample and the date and place of collection. They also require all tubes to be sealed, secured, and transported to the laboratory $\leq$15 d after withdrawal. In Oregon and South Dakota, the relevant regulations also require that all samples be refrigerated when they arrive at the laboratory, to maintain sample integrity—a requirement that no other states impose explicitly.

In Georgia and Virginia, once the collection tube arrives at the laboratory, the staff must complete and file a form that identifies the person receiving the sample, the date of receipt, and a statement that the seal on the tube has not been broken or tampered with. Samples may then be divided, labeled, and stored to ensure their integrity, with the remainder of the sample being kept for possible retesting or updating of the original analysis. These requirements, however, are described as procedural—not substantive—so that substantial compliance with them is all that is required.

Nature of Analysis Authorized and Quality-Control Provisions

Statutes vary considerably in the specificity with which they describe the nature of the analysis that can be performed on samples collected for data banks. Most refer simply to "DNA analysis" or "genetic marker" testing for "individual identification" purposes. Statutes in states where the collection of saliva, in addition to blood, is authorized often also typically refer to tests for secretor status. Oregon's statute permits the use of "all techniques that the department of state police determines are accurate and reliable in establishing identity," including but not limited to comparative DNA analysis and the study of cell-surface antigens, polymorphic enzymes, and polymorphic proteins (Or. Rev. Stat. §§181.085, 137.076, and 161.325). The new bill under consideration in Massachusetts refers to "any test that determines the DNA composition of a sample," including but not limited to "DNA fingerprinting," "DNA print identification," "genetic fingerprinting," or "restriction fragment length polymorphism" (Mass. Senate bill 685, 1993).

California's statute was amended in 1989 and now permits genetic typing only for those markers having value for law enforcement purposes; some of the new bills now under consideration in other states also contain this limitation. The California statute is one of the few existing laws that require the responsible agency to conduct peer review and validation studies and to publish its DNA analysis procedures.

The data-banking laws contain very few directives regarding quality control or quality assurance. Of the statutes already enacted, currently only those in Kentucky, Missouri, and Washington explicitly require that the analysis methods and/or computer software used be compatible with the FBI's procedures to facilitate data exchange on a national level. Some of the new bills under consideration in other states also contain this requirement. Of course, strong incentives for uniformity exist even in the absence of such a statutory mandate, since most laboratories will presumably be eager to do what is necessary to facilitate the exchange of DNA data on an interstate level.

Missouri and Washington have established special procedures designed to help ensure compliance with quality-control standards by local law-enforcement agencies within the state that seek to use their networks. In those states, no local law-enforcement agency can establish or operate a data bank unless its equipment is compatible with that of the state system and unless it is equipped to receive and answer inquiries from the state data bank and the FBI. In addition, those states prohibit local law-enforcement agencies from receiving information from the state data bank unless their procedures and rules for the collection, analysis, storage, expungement, and use of DNA data are consistent with the procedures and rules applicable to the state system and the FBI. The bill pending in North Carolina would mandate similar quality-control standards.

Resources and Authority to Contract for DNA Analysis

To date, few states appear to have appropriated adequate funds for personnel, laboratory space, equipment, and supplies to support their data-banking legislation. As mentioned, financial constraints led Louisiana to discontinue its data-banking efforts. Other states employ a variety of mechanisms to fund their operations. The Oregon and South Dakota statutes require offenders to contribute to the costs of sample collection and/or testing; legislation now pending in Arizona and Massachusetts, as well as one of several new bills introduced in Texas, would also require this. Exceptions may be made, however, if the offender is indigent. Other states assess a charge on individuals seeking to access information in the data bank. The proposed bill in Vermont, for example, would allow laboratories to charge out-of-state law-enforcement agencies a reasonable fee for searching its data bank.

Limited staff and laboratory capacity may make the analysis of all collected samples by the responsible agency difficult, if not impossible, in many states. Some states have anticipated this problem by including within their statutes provisions that expressly authorize crime laboratories to contract with qualified independent laboratories for DNA analysis services. One of the bills now under consideration in Texas would also allow contracting with an institution of higher education, but it would specifically require all contractors to adhere to the FBI's quality-assurance standards and to produce analysis results that meet the FBI's acceptance criteria.

Retention and Expungement of Samples and Data

Few statutes directly address the question of whether the tissue samples from which DNA is extracted must be retained along with the resulting profiles—and, if so, for how long. An exception is Michigan, where samples from offenders must be retained permanently but where samples from suspects (persons who are investigated or prosecuted but not ultimately convicted) need only be kept as long as needed for the case. Florida's law, as well as the new bills pending in North Carolina and Texas, expressly require retention of samples, but they do not specify how long they must be stored. In Oregon, while the enabling statute does not address the duration of sample retention, administrative regulations make clear that the responsible agency may discard samples after they have been analyzed.

A small but growing number of laws specify a formal mechanism for expunging data-bank information on offenders who prove to have been wrongly convicted (or accused) and whose cases (in connection with which the sample was taken) are dismissed (see table 10). Such procedures typically require the responsible agency to purge all samples and identifiable data when it receives both a written request for expungement and a certified copy of the court order reversing and dismissing the conviction. However, Oregon's law, which contains especially detailed expungement provisions, states that the mere setting aside of a conviction (as distinct from outright reversal) is not a basis for expungement.

California's statute, while silent on the matter of expunging the records of offenders whose convictions are overturned, provides that *crime scene* evidence accumulated with respect to a person who is in the data bank solely as a result of a criminal *investigation* must be stricken from the data bank when it is determined that he or she is no longer a suspect. A new bill pending in Delaware would require the responsible agency to provide the state police, on a regular basis, with an

Table 10

Provisions for Expungement under Existing DNA Forensic Data-banking Laws

State	Yes	No
Arizona		X
California		X
Colorado		X
Florida		X
Georgia	X	
Hawaii		X
Illinois		X
Iowa		X
Kansas		X
Kentucky	X	
Michigan		X
Minnesota		X
Missouri		X
Nevada		X
Oregon	X	
South Dakota		X
Tennessee		X
Virginia	X	
Washington	X	

updated list of names of persons whose profiles are in the data bank.

Access by Offenders, Challenges to Accuracy, and Admissibility of Data

Apart from the general statements in a few statutes that the responsible agency should "strive to maintain or disseminate only accurate and complete records," most statutes do not include specific procedures to ensure the accuracy of profiles in the data bank. However, legislation being proposed in Texas would specifically require the responsible agency to develop biennial plans to improve the reporting and accuracy of that state's data bank and to develop and maintain monitoring systems capable of identifying inaccurate or incomplete information.

Only a couple of statutes directly address the question of access to samples or data by offenders or their defense counsel. Oregon's law has the most detailed provisions on offender access; it expressly permits offenders, on request, to inspect DNA data relating to themselves. The responsible agency in Oregon has issued regulations establishing detailed procedures for inspecting DNA samples and data and for challenging the accuracy of records, taking into account the need to preserve the materials from contamination and destruction. However, the agency can deny inspection if it determines that there is a "reasonable likelihood" that inspection would prejudice a pending criminal investigation. In addition, neither the offender nor counsel may independently test samples. No statutes expressly recognize a right of a defendant to conduct a full search of the data bank to determine whether someone else in the data bank (e.g., a relative with a similar DNA profile) might have committed the crime in question.

The California statute, as well as some of the new bills now pending in other states, expressly permit the disclosure of DNA data to defense counsel, in compliance with discovery. However, these laws neither contain detailed provisions on offender access nor recognize a right to challenge the accuracy of data. It is also unclear whether the right of access contemplated by the California statute applies to data in the *offender* data bank or only to data derived from *evidence samples* that have been banked and are later sought to be introduced as direct evidence in court.

Questions about offender access to samples or data and about procedures for challenging the accuracy of information are most likely to arise when the state seeks to use in court information from the data bank. No laws, however—with the exception of Virginia's—explicitly authorize the admissibility in court of DNA data *collected specifically for the data bank.* Most states seem to contemplate using the data bank solely to generate investigative *leads;* presumably, if a suspect were identified on the basis of a data-bank profile, a new sample would be drawn, and it is only that sample that would be introduced as evidence. Even this is not entirely clear, however, because most statutes are silent on the precise procedures to be followed when a "match" occurs through the data bank. The new bills under consideration in Delaware and Massachusetts, as well as one of the pending bills in New York, would expressly make all DNA data—whether derived from samples collected for the proposed offender data bank or derived in the course of ordinary casework—automatically admissible in all court proceedings. California's statute permits the inclusion, in transcripts or records of court proceedings or in other public records, of information from its data bank, when this is authorized by a court decision or other law.

Confidentiality of Identifiable DNA Information

Data-banking statutes vary widely in the detail with which they address informational privacy and access to

individually identifiable DNA samples and data. California's law, as well as some of the bills pending around the country, incorporates reasonably strong confidentiality safeguards. A number of states expressly mandate that all DNA data be "securely stored" and "remain confidential," or they require that the collection, processing, maintenance, and dissemination of DNA and DNA data be done with regard to privacy interests of individuals.

Oregon has one of the more detailed laws on third-party access. Its statute prohibits the disclosure of any "sample, autoradiograph, physical evidence or criminal identification information obtained, stored, or maintained under authority of [the data-banking law] *except* to a law-enforcement agency or district attorney in the course of a criminal investigation or proceeding, to a party in a criminal or juvenile proceeding if disclosure is required by a separate statutory or constitutional provision, or to a court or grand jury in response to a subpoena or court order when the evidence is not otherwise privileged [emphasis added]" (Or. Rev. Stat. §§181.085, 137.076, and 161.325). The Oregon statute is unique in prohibiting redisclosure by any public agency to whom an original disclosure was made.

Washington's law recognizes that special risks to privacy may be implicated when some researchers (e.g., criminologists searching for correlations between alleles and certain behavioral traits) seek access to DNA data. The responsible agency there has issued regulations to prohibit the use of DNA data for any research or other purpose that is not related to a criminal investigation or to improving the operation of the system.

The proposed bill in North Carolina would allow DNA data to be made available on receipt of an official court order directing release of the information to other "appropriate parties," but only after a court hearing. The responsible agency would also be required to maintain a file of all such court orders.

Some laws say little on the question of informational privacy and do not ensure that *only* law-enforcement agencies can obtain those data. In such states, disclosures could arguably be made to persons or agencies outside law-enforcement, without technically violating the law.

Relationship to Other Information-Practices Laws

In practice, the degree to which information in a data bank can be accessed by third parties depends on the interplay between the state's data-banking statute and other laws governing information practices. Almost all states have laws that regulate access to public and criminal history records; these laws vary greatly among states. Some data-banking statutes explicitly address the possible interplay with these other laws.

For example, Florida and Kentucky specifically exempt from the provisions of their open-records laws any DNA data collected for the data bank; the new bill under consideration in Delaware would also do this. California and Florida prohibit the inclusion, in their centralized repositories for criminal history records, of any DNA data from the data bank. Proposed legislation in Texas would both prohibit the inclusion of criminal history information in the data bank *and* exempt from the state's open records law the data-bank information. Nevada, on the other hand, *requires* the submission of *all* DNA profiles to its criminal justice–information repository.

Most existing statutes are altogether silent on the question of whether computerized DNA information in the data bank can be included in automated criminal–records systems or be made subject to other open-records laws. In such places, as well as in other states where other privacy laws are uncertain in application, the practical extent to which DNA data can be shielded from third-party access is unclear. In general, DNA data seem likely to move into increasingly wider access.

Methods of Requesting DNA Data and Release of Anonymous Data

Few laws outline the permissible procedures for making requests for individually identifiable DNA data. The statutes and bills that do address this matter typically provide that requests may be made only by personal contact, mail, or electronic means. These states also require the responsible agencies to adopt procedures for verifying the identity and authority of any person or agency requesting data-bank information.

In some states, only when an evidence sample matches a profile in the data bank can either the existence of the data in the data bank be confirmed or identifying information be released. These states also require that both the name of the requester and the purpose for which the information was sought be recorded and furnished to the offender, on request.

States that authorize the use of their data banks for the generation of population statistics generally permit the release of *anonymous* DNA data (data that cannot be associated with an identifiable individual) to persons other than those directly involved in law enforcement. Thus, in California, disseminating statistical or research

Table 11

Penalties for Unauthorized Release, Receipt, or Use of DNA Data under Existing DNA Forensic Data-banking Laws

State	Unauthorized Release	Unauthorized Receipt or Use
Arizona		
California	X	
Colorado		
Florida		
Georgia	X[a]	X[a]
Hawaii	X	X
Illinois		
Iowa		
Kansas		
Kentucky	X	X
Michigan		
Minnesota		
Missouri		
Nevada		
Oregon		
South Dakota		
Tennessee		
Virginia	X[a]	X[a]
Washington		

[a] Also covers DNA samples.

information from the data bank is permitted as long as the subject is not and cannot be identified from the information disclosed. On the other hand, in Georgia and Virginia, disclosure of even anonymous DNA data is expressly limited, to those in law enforcement.

The new bill pending in North Carolina would permit the sharing of population statistics with "other law enforcement agencies, crime laboratories that serve them, or other third parties [deemed] necessary to assist . . . with statistical analysis," as well as to other agencies participating in the FBI's identification system (N.C. House bill 1050, 1993). In addition, it would allow the release of anonymous data to other DNA laboratories to support identification research and protocol development for forensic DNA analysis or for quality-control purposes. Some of the other new pending bills contain similar provisions.

Penalties for Unauthorized Disclosure of DNA Samples and Data

Currently, only five states provide statutory penalties for the unauthorized disclosure of DNA data (see table 11). In these states, as well as under the bills pending in Delaware, New York, North Carolina, and Texas, the knowing, intentional, or, in some cases, "willful" disclosure of DNA data, either to unauthorized individuals or agencies or for other than law-enforcement purposes, constitutes a misdemeanor. With one exception, each of these states also makes (or will make) it a misdemeanor to receive or use (or, in some cases, to *attempt* to use) DNA data without authorization.

Only a few statutes explicitly address the question of penalties for unauthorized release or use of *samples* (as distinct from data). In Georgia and Virginia, obtaining or attempting to obtain samples without authorization is a felony.

Role of DNA Advisory or Review Committees

None of the states that have enacted data-banking laws appear to have set up statutory licensing systems for their DNA forensic laboratories. However, in Florida, a companion statute to the data-banking law creates a crime-laboratory council consisting of crime-laboratory directors, the president of the state attorney's association, the attorney general (or designee), and a medical examiner and criminal court judge appointed by the governor. The statute directs this council to issue recommendations regarding a wide range of matters, including the development of guidelines and standards for the inclusion of additional laboratories into the state crime-laboratory system, the evaluation of forensic science training and development programs, and consideration of laboratory safety and health issues.

Similarly, Michigan's data-banking law requires the establishment of a state DNA advisory committee consisting of law-enforcement officials, forensic scientists, defense attorneys, and judges. This committee will advise the state legislature regarding a variety of concerns, including effective coordination of the rules and regulations governing forensic DNA laboratories with law-enforcement agencies, courts, prosecutors, and defense counsel; recommendations to ensure the availability of reliable forensic DNA testing to law-enforcement agencies, prosecutors, and counsel for indigent defendants; regulations to protect the privacy rights of individuals subject to the data-banking law; and recommendations for external and internal proficiency-testing systems, for the regular testing of methodologies and procedures. This committee, however, has not yet been formally convened, because Michigan's data-banking law cannot take effect until the state legislature appropriates sufficient money to fund it—an event that has not yet occurred.

One of the two major competing bills in New York —known as the "governor's program bill"—will, if enacted, mandate the establishment of a "forensic science review panel." That bill (similar to another new bill pending in Texas) will also require the convening of a panel subcommittee for the review and evaluation of accreditation standards for forensic DNA analysis methods. However, the governor's program bill (which currently has the support of the state senate but not of the state assembly) would essentially keep oversight over state DNA forensic analysis and data-banking activities with law-enforcement itself. The chief competing New York bill (which mirrors the recommendations made by the National Academy of Sciences and which has support in the state assembly but not in the state senate) would establish a primarily *civilian* scientific review board and DNA advisory committee. The committee proposed in that bill would also have somewhat more expansive functions than those provided in the governor's program bill; for example, it would be required to propose recommendations for protecting the privacy rights of persons whose DNA profiles are to be included in the data bank. The controversy over who should be in charge of setting quality-assurance and privacy standards for DNA data banks—i.e., whether standards should be set by law-enforcement agencies regulating themselves or by mixed regulatory panels composed of outside experts (e.g., scientists, ethicists, and lawyers)—has also been a source of considerable debate on the federal level, in connection with the FBI's proposed regulatory role under the DNA Identification Act of 1993 (H.R. 829, S. 497, 103d Cong., 1st sess.).

Discussion

The Rapid Expansion of DNA Data Banking and Possible Retroactivity Problems

DNA data banking for forensic purposes, while still in a start-up period, is clearly here to stay. Virginia's data bank, which is currently the most active, has already collected 80,000 samples from convicted felons, and it is analyzing them at the rate of 1,500–2,000/mo (P. Ferrara, Director Virginia Division of Forensic Science, personal communication). Continuing technological refinements, coupled with the large number of criminal convictions that occur each year (750,000 felonies in the United States), virtually ensure that the number of DNA profiles in forensic data banks across the country will soon far exceed the number in the various small repositories kept by clinical researchers in connection with their study of particular genetic disorders.

Accompanying the dramatic growth in the number of DNA forensic data banks during the past 3 years has been a marked expansion in the scope of the population that they are designed to target. Originally aimed only at persons convicted of serious sex offenses, a number of laws now authorize the taking of samples from all or most convicted felons—or even, in some cases, from those convicted only of certain misdemeanors.

The justification for taking samples from serious sex offenders or other violent felons is based on the fact that persons who commit such crimes are often repeat offenders. According to a 1989 Bureau of Justice Statistics report, an estimated 62.5% of those released from prisons are rearrested for a felony or serious misdemeanor in $\leq$3 years (United States Department of Justice, Bureau of Justice Statistics 1989). Of those in the study who were imprisoned for violent offenses and who subsequently were released, 59.6% were rearrested for a similar offense in $\leq$3 years. Rates of recidivism for rapists are especially high. Released rapists in the study were 10.5 times more likely than other felons to have a subsequent arrest for rape, and prisoners who had served time for other sexual assaults were 7.5 times more likely to be arrested for a sexual assault than convicted felons who had not served time for sexual assault. Other violent offenders also have high recidivism rates. For example, those released after serving time for murder or nonnegligent manslaughter were nearly five times more likely than other prisoners to be rearrested for homicide.

In 1991 there were 106,593 reported forcible rapes, of which only 51.8% were cleared by arrest (United States Department of Justice, Bureau of Justice Statistics 1991). This statistic, coupled with the findings on recidivism, provides a compelling argument for banking DNA data on serious sex offenders and other violent felons. The ability to compare evidence samples with these profiles can help to link related cases, track the activities of serial rapists or murderers, and exonerate the innocent. Rapes and murders are also the types of crimes in which biological evidence from the offender (in the form of semen or blood) is most likely to be found. They also are often crimes in which no suspect can be identified or in which eyewitness testimony is unreliable. Thus, it is reasonable to include in DNA data banks DNA samples from these serious offenders.

On the other hand, the current trend toward includ-

ing an ever-expanding range of offenders—including nonviolent felons and even some misdemeanants—has much less justification. Minor sex offenses such as lewd and lascivious behavior, as well as property crimes such as arson or robbery, do not tend to be associated with biological evidence. Including within a data bank the DNA from persons convicted of such offenses might make sense if most tended to move on to commit other, more serious offenses, of types that are associated with biological evidence—but little evidence exists to support this. Statistics show that only 0.4% of nonviolent felons are later arrested on rape charges; only 0.8% are arrested for murder (United States Department of Justice, Bureau of Justice Statistics 1989).

The inclusion of juveniles within the scope of many data-banking laws raises unique privacy concerns but can arguably be justified on the basis of statistics showing that juvenile delinquency often foreshadows adult crime and that the more serious the juvenile career, the greater the chances of adult criminality (United States Department of Justice, Bureau of Justice Statistics 1987). The same is probably true for the increasing inclusion, within the purview of some laws, of transferees from prisons in other states, since more than one of every eight rearrests occurs in a state other than the state of release (United States Department of Justice, Bureau of Justice 1989). Again, however, to the extent that crimes other than either serious sex offenses or other violent crimes are encompassed, the rationale for including juveniles or transferees convicted of those offenses is questionable. In addition, with juveniles (and with arrestees, such as those from whom samples are collected for South Dakota's data bank), questions may be raised about whether the DNA profiles should be retained permanently or expunged after a period of time. Nonetheless, one court has already upheld Minnesota's practice of retaining DNA data on juveniles, over the claim that it conflicts with the policy of maintaining the privacy of juvenile-court records (Matter of Welfare of ZPB, 492 N.W.2d 651, Minn. App. [1991]).

The FBI legislative guidelines stress the need for legislatures to assure that their data-banking statutes seek to accomplish a legitimate state interest; they specifically state that misdemeanants, for example, should not be included (United States Department of Justice, Federal Bureau of Investigation 1991). The inclusion of too many offenders within the purview of a data-banking statute may make that law subject to challenge, on the basis that it violates the Fourth Amendment prohibition against unreasonable searches and seizures. Although one early decision rejected a similar argument, in upholding Virginia's data-banking law (Jones v. Murray, 962 F.2d 302 4th Cir. [1992]), that opinion was issued over a vigorous dissent and is not binding on courts in other areas of the country. A more recent state court decision upholding another state's law (Washington's) suggests strongly that the constitutionality of a data-banking law depends on how closely the class of persons on which it is designed to operate has been tailored to the data bank's purpose (Washington v. Olivas, 856 P.2d 1076 S. Ct. Wash. [1993]). Future challenges to other states' data-banking laws, on the grounds of overbreadth, thus seem likely.

Another area where legal challenges to DNA forensic data-banking legislation seem likely is the matter of retroactivity. As discussed, in most states the requirement that offenders provide a sample for data banking applies not only to those who are convicted after the statute's effective date, but also to those who were already in prison. In one case so far, inmates argued that such a requirement interfered with a vested liberty interest and violated the constitution's ex post facto clause (the provision that prohibits changing the punishment for a crime or inflicting a greater punishment than applied when it was committed) (Jones v. Murray, 962 F.2d 302 4th Cir. [1992]). While the court did not fully accept this argument, it did invalidate the statute to the extent that it could be interpreted as authorizing a modification of the state's mandatory parole period (by holding beyond their established release dates—and without valid process—prisoners who refused to provide samples). Lawsuits contesting the retroactive application of other statutes will almost certainly be brought.

Quality Assurance, Standards for Admissibility, and Analysis Methods

Quality assurance and quality control are crucial concerns for DNA forensic analysis generally—not just for DNA data banking. Nevertheless, the finding that so few of the data-banking laws explicitly address these matters is troubling. Also troubling is the fact that none of the states with data-banking laws have set up statutory licensing systems for their DNA forensic laboratories, despite the recommendation in the National Academy of Sciences (1992) report that they do so.

Should the federal DNA Identification Act of 1993 (H.R. 829, S. 497, 103d Cong., 1st sess.) become law, states will be required to adopt uniform data-banking procedures to maintain their eligibility for federal

grants; they also will be required to adhere to specified quality-assurance and proficiency-testing requirements (DNA Identification Act of 1993, H.R. 829, S. 497, 103d Cong., 1st sess.). However, the adequacy of the current Technical Working Group on DNA Analysis Methods quality-assurance guidelines that the FBI endorses has been called into question (National Academy of Sciences 1992), and to the extent that the DNA Identification Act entrusts the FBI, rather than a separate agency, with oversight over DNA forensic testing laboratories, challenges to the quality of the DNA data being generated for data banking will probably continue to be raised. For example, expert reports submitted to the court in United States v. Yee (134 F.R.D. 16 N.D. Ohio [1991]) documented serious deficiencies in the autorads within the FBI's own DNA data bank, which the FBI acknowledged and corrected only reluctantly (United States v. Yee, 134 F.R.D. 16 N.D. Ohio [1991]). Unacceptably high laboratory error rates in forensic areas *other than* DNA testing, as well as the reluctance of many crime laboratories to commit themselves to meaningful self-regulation, have also been documented (Jonakait 1991).

Of course, DNA profiles held in a data bank are unlikely *themselves* to be offered as direct evidence in court—a fact that might at first seem to make the absence of strict statutory quality-control provisions for creating data-bank profiles less problematic. Indeed, the FBI legislative guidelines recommend, and most statutes seem to contemplate, that, when a putative match occurs between an evidence profile and a profile in a DNA data bank, this merely gives rise to probable cause to draw a new sample from the suspect to confirm the match. It is the profile derived from this new sample—and not the profile from the data bank—that would then be introduced into court as evidence to support subsequent prosecution (United States Department of Justice, Federal Bureau of Investigation 1991).

Nevertheless, poor quality assurance in the set-up of data banks is unacceptable. First, it can result in false negatives, steering the investigation away from the real perpetrator(s) and confounding law enforcement. Second—and more important from a civil-liberties standpoint—it can create a large number of false leads, resulting in intrusive "sweeps" that harm innocent persons. This is because CODIS currently contemplates doing initial searches with just two or three probes and using a larger match window than is used to size bands in ordinary casework. As a result, searches are likely to generate lists of several potential suspects—not a perfect "hit" that points conclusively to a single person. Indeed, the larger the data bank (i.e., the more offense categories that are included), the greater the number of individuals who will be targeted for further investigation—which, as a practical matter, usually means further drawing of blood. Sloppiness in creating data-bank profiles will increase this imprecision, resulting in even longer lists of potential suspects and the possibility of even broader "sweeps."

The matter of quality control with respect to *evidence* samples analyzed for the data bank (in states where the statutes actually contemplate the banking of such profiles) raises even greater concerns. For evidence samples, quality control is paramount, since the profiles derived therefrom may be presented in court. The trend in the courts has been toward admitting DNA profiles done on evidence samples and on samples taken from suspects to confirm a match (subject, of course, to challenges to reliability and to the population statistics that form the reference base for any asserted probability calculations). However, a major weakness in many statutes is their failure to distinguish, for purposes of admissibility, between DNA analyses performed in connection with ordinary casework (i.e., profiles of evidence samples and of samples from suspects for comparison) and profiles done for the convicted offender data bank.

Another flaw in most data-banking statutes is their failure to specify (as, e.g., California's law does) that DNA analysis on samples collected for the data bank can be done *only* for those markers having value for law-enforcement purposes (i.e., relating to individual identification). This could create problems in the future, particularly if DNA technology progresses to the point where direct testing for a wide range of genetically influenced behavioral traits becomes possible. The general statement in most laws—i.e., that the data banks are to be used for "law enforcement purposes"—seems insufficient to preclude the possibility of such misuse.

Retention of Samples and Data

A particularly controversial issue in DNA forensic data banking relates to whether crime laboratories should be allowed to retain tissue samples once they have been analyzed, as opposed to merely retaining the resulting DNA profiles. The American Society of Human Genetics Ad Hoc Committee on Individual Identification by DNA Analysis has concluded that it is appropriate for laboratories to retain samples, so long as

adequate rules of disclosure and access are implemented (Ad Hoc Committee on Individual Identification by DNA Analysis, The American Society of Human Genetics 1990). However, critics have expressed concerns that, if samples are preserved, they could be reanalyzed, perhaps many years later, to answer questions far different than the original question of identity (Ballantyn et al. 1989).

Here, a distinction exists between an evidence sample gathered in the course of a routine investigation and a sample taken from a convicted offender specifically for the data bank. An evidence sample obviously must be retained until the case is closed, to ensure its availability for court use. However, for samples taken from convicted offenders, little reason for retention exists. On the assumption that adequate quality-control measures are used in creating the data-bank profile, it should rarely be necessary to go back to an original sample for retesting. If a putative match occurs, it can be checked easily by drawing a new sample from the suspect and running it against the evidence sample.

A crime laboratory might, of course, be able to claim an interest in going back to original samples to reanalyze them by using better, more sophisticated probes that may, in the future, become the state of the art. This argument, however, may prove too much: If the technology evolves so that current analysis techniques become obsolete or so that different probes become the standard, none of the profiles being entered into data banks using today's probes will any longer be useful for making matches with future evidence samples analyzed with the newer methods. The suggestion that *all* of the samples that have been and are today being analyzed will need to be reanalyzed at some later date suggests, in turn, that large-scale data banking at the present time is, in fact, premature—or, at least, highly inefficient.

Regardless of whether samples are saved, states should permit persons whose profiles are included in the data bank to seek expungement of the data, as well as expungement of the sample itself, if the case against them is later reversed and dismissed—a procedure that few statutes now allow. It may also be desirable to permit offenders or their defense counsel to inspect their own DNA profiles (or independently to search the data bank), although, here again, a distinction between suspects who are actually being prosecuted on the basis of information in the data bank and convicted offenders whose profiles are in the data bank solely to generate future investigative leads may be warranted. In the first case, access to the samples and to the data should be permitted as a part of routine discovery. In the later case, detailed access provisions (such as those contained in Oregon's law) are probably not as crucial—at least if it is assumed, as the FBI legislative guidelines contemplate, that the banked profile will not itself be used in court (United States Department of Justice, Federal Bureau of Investigation 1991).

Third-Party Access to Samples and Data

One of the concerns about DNA forensic data banking that is most frequently expressed by critics of the practice is the risk that information in the data banks will fall into the hands of third parties—such as insurance companies, employers, schools, and others—who will use it to discriminate unfairly against individuals (DeGorgey 1990). Most of the existing statutes contain at least some protection against this possibility, by providing generally for the confidentiality of individually identifiable DNA samples and data. Only a few, however, provide criminal penalties for its unauthorized disclosure or use. This is a major gap in many laws. If enacted, however, the DNA Identification Act of 1993 (H.R. 829, S. 497, 103d Cong., 1st sess.) will mandate the imposition of fines ≤$100,000 for those who "willfully" disclose or obtain DNA information without authorization.

In assessing the potential for improper disclosures, a distinction between the *tissue samples* collected for the data bank and the *data* (i.e., profiles) that are derived from them should be recognized. The release of DNA data currently poses only a limited risk to privacy, because the profiles generated with the probes now being used contain no information relating to disease or behavioral characteristics. This could change, however, especially in light of the recent finding that short, highly repetitive sequences of DNA reside near and may influence clinically important genes (Richards and Sutherland 1992). To guard against the possibility of misuse of DNA data that someday may become associated with disease genes (or with behavioral traits), sophisticated computer security measures and data-encryption techniques that make it more difficult to associate a particular individual with a given profile will be essential.

A more serious risk to privacy in DNA forensic data banking is implied by the possible misuse of *samples*. As discussed above, unlike profiles—which, at least for the present, contain little information likely to be of interest to those outside law enforcement—samples carry a potential wealth of information. Some of the concerns expressed about the potential for misuse of samples

may be overstated; for example, it is unlikely that an insurance company anxious to discover an applicant's predisposition to genetic disease would use so roundabout a method to obtain a blood sample for testing, when it can easily request one directly from the applicant.

On the other hand, a realistic risk does exist that researchers will seek access to samples—for purposes unrelated to law enforcement that many would regard as controversial. For example, for a behavioral geneticist or criminologist researching possible genetic predispositions to violence or pedophilia, a ready-made repository of tissue samples from thousands of convicted felons could seem invaluable. Requiring the destruction of samples after they have been analyzed for the data bank would greatly reduce the risk of their misuse by researchers or by other third parties. At the least, safeguards should be instituted to ensure that no samples are made available for research use unless the research protocols have been approved by an institutional review board.

Other Privacy Concerns

Even if it is assumed that adequate safeguards exist to ensure that samples and data will not fall into the "wrong hands," DNA forensic data banking raises other, more fundamental privacy concerns. What, exactly, *is* "law enforcement"? Does it encompass immigration authorities, child support–enforcement officials, or other state agencies, which may someday all be connected through massive interlocking computer networks? Already, the U.S. Department of Defense has begun to acquire blood and saliva samples from all military recruits, to assist in the identification of remains thought to be those of MIAs. More than 121,000 samples have been collected since 1992, with another 1,500 samples coming in every day (Bowman 1993). The military plans to extract DNA from these samples only as the need arises; for example, if a platoon were decimated by a missile attack, the tissue stored on members of that platoon would be analyzed for comparison with the remains. Despite these currently limited objectives, the military's efforts will almost surely help to expand interest in DNA identification technology in society at large.

As DNA identification techniques improve, economies of scale will undoubtedly reduce testing costs and facilitate adaptation of the technology to a variety of new populations (Annas 1993). Will state DNA forensic data-banking laws, which started out as laws narrowly directed at repeat sex offenders but that are increasingly being broadened to include other categories of crimes, gradually open the way to a "surveillance creep," so that eventually *everyone* will be required to "give blood for the government?" These and related questions merit increased public and professional consideration.

Conclusion

DNA forensic data banking is growing rapidly, but, so far, surprisingly little attention has been paid to how it is being conducted or to its implications for society. The benefits of data banking must be balanced against the potential threat to privacy and civil liberties that is entailed when the government begins to amass large quantities of DNA from its citizens. So far, the technology for the collection, storage, analysis, retrieval, and use of DNA data has far outpaced the attention paid to the need to safeguard these interests.

We found much variation among data-banking laws and conclude that, while DNA forensic data banking carries tremendous potential for law enforcement, many states, in their rush to create data banks, have paid little attention to issues of quality control, quality assurance, and privacy. In addition, the sweep of some laws is unnecessarily broad. Legislative modifications are needed in many states, to better safeguard civil liberties and individual privacy. Although the FBI legislative guidelines provide guidance for lawmakers in a number of areas, privacy concerns might be more carefully addressed if The American Society of Human Genetics and other appropriate organizations commented on the issues.

Empirical data that document how crime laboratories are actually setting up and running their data banks are also needed. The results of a recently completed survey of crime-laboratory personnel, regarding their data-banking activities, will be the subject of a future article.

Acknowledgments

This work was supported in part by the Human Genome Project, Department of Energy grant DE-FG02-91ER61237, MCH grant MCJ-259151-02-0, ADD grant 90 DD 0213, and Department of Mental Retardation of the Commonwealth of

Massachusetts grant 1000-10003-SC. We also acknowledge the support of Boston College Law School.

References

Ad Hoc Committee on Individual Identification by DNA Analysis, The American Society of Human Genetics (1990) Individual identification by DNA analysis: points to consider. Am J Hum Genet 46:631–634

Anderson C (1992) Courts reject DNA fingerprinting, citing controversy after NAS report. Nature 359:349

Annas GJ (1993) Privacy rules for DNA databanks. JAMA 270:2346–2350

Ballantyn J, Sensabaugh G, Witowski J (eds) (1989) DNA-technology and forensic science. Banbury rep 32. Cold Spring Harbor Laboratory, Cold Spring Harbor, NY

Bowman T (1993) Research on DNA could solve a host of problems for military. Houston Chronicle (July 25)

DeGorgey A (1990) The advent of DNA databanks: implications for information privacy. Am J Law Med 16:381–398

Jonakait RN (1991) Forensic science: the need for regulation. Harvard J Law Technol 4:109–191

National Academy of Sciences, National Research Council, Commission on Life Sciences, Board of Biology (1992) DNA technology in forensic science. National Academy of Sciences, Washington, DC

Richards RI, Sutherland GR (1992) Dynamic mutations: a new class of mutations causing human disease. Cell 70:709–712

Roberts L (1991) Fight erupts over DNA fingerprinting. Science 254:1721–1723

Technical Working Group on DNA Analysis Methods (1989) The combined DNA index system (CODIS): A theoretical model. Federal Bureau of Investigation, Quantico, VA

United States Congress, Office of Technology Assessment (1990) Genetic witness: forensic uses of DNA tests. OTA-BA-438. US Government Printing Office, Washington, DC

United States Department of Justice, Bureau of Justice Statistics (1989) Recidivism of prisoners released in 1983. US Government Printing Office, Washington, DC

——— (1987) Recidivism of young parolees. US Government Printing Office, Washington, DC

——— (1992) Sourcebook of criminal justice statistics 1991. US Government Printing Office, Washington, DC

United States Department of Justice, Federal Bureau of Investigation (1991) Legislative guidelines for DNA databases. Federal Bureau of Investigation, Quantico, VA