Chapter 5

Computer Technology and Informational Privacy

"Just the mention of one name can clarify the need for the nationwide exchange of criminal history data including DNA information: Ted Bundy, recently executed killer whose heinous crimes spanned the nation.'

William S. Sessions, Director
Federal Bureau of Investigation
Feb. 20,1989

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

Justice Brandeis
Dissenting Opinion
Olmstead V. *U.S.* **277** U.S. 438,479 (1928)

CONTENTS

Page

CURRENT COMPUTER APPLICATIONS 114
Restriction Fragment Length Polymorphism Analysis 114
Computers and Polymerase Chain Reaction 117
Computers in Court: Cost-effectiveness 118
DATABASE CONSIDERATIONS 120
Types of Databanks 120
Technical Considerations 124
Database Management 125
DATABANKS AND INFORMATIONAL PRIVACY 128
Who Will Be Tested? 129
What Do the Tests Reveal? 131
How Will DNA Information Be Stored? 132
Who Will Have Access to DNA Information? 133
Investigatory Use of Population Statistics 134
FINDINGS AND SUMMARY 136
CHAPTER 5 REFERENCES 136

Boxes

Page

5-A. Automated Fingerprint Identification Systems 1141
5-B. The Social Security Number a sa National ldentifier 115
5-C. Existing Storehouses of Genetic Information 121
5-D. Newborn DNA Typing 131
5-E. The Leicester Case: DNA's Criminal Debut 135

Figures

Page

5-1. DNA Sizing Portrayed Through Autoradiography 116
5-2. Autoradiography :The Importance of X-ray Film Exposure 117
5-3. Semiautomated Analysis of DNA Autoradiogram 118
5-4. Description of the FBI's Computerized DNA Analysis System 119
5-5. DNA Variation Among Population Groups 122
5-6. DNA Typing: Reported Uses and DNA Databank Legislation by State 123
5-7. Proposed Data Files: Who Will Maintain Them? 127
5-8. How a Database of DNA Information Could Be Created and Used 130

Chapter 5

Computer Technology and Informational Privacy

Computer technologies enhance the ability of Federal, State, and local agencies to uncover wrongdoing at many levels: Entitlement program administrators use computer matching to catch people who abuse welfare, the Internal Revenue Service compares individual returns with information provided by banks to discover where taxes on interest have been underpaid, and the automated fingerprint identification system (box 5-A) has revolutionized the ability ofcriminal investigators to identify suspects within and across jurisdictional boundaries.

Applications of these computer systems raise issues of informational privacy. Linkage of information in a variety of public and private sources is creating a de facto national database containing information on most Americans (53). (The term de facto is used to distinguish the database from one created by law, i.ea de jure national database.) Social security numbers (SSN) often link these databases, and the SSN has become a national electronic identifier (box 5-B) even though some attempts have been made to control its use. Use or misuse of personal information collected in electronic databases can affect an individual's ability to obtain employment, credit, insurance, and other services and benefits (e.g., housing or Aid to Families With Dependent Children).

Federal, State, and local criminal justice agencies now express considerable interest in using computer technologies to improve their abilities to analyze and share the results of DNA tests. Advanced image analysis technologies, which combine the attributes of video and computational machines, coupled with databases compiled from test results, can meet the needs of forensic scientists using DNA typing to:

- **generate** population statistics,
- . aid the technician in the identification of band position, and
- compare the results of different tests.

When experts use DNA tests to confirm the identity of a child's parent or to confirm that a suspect is the source of crime scene evidence, they declare a match or nonmatch between DNA specimens. In the case of a match, they also express the probability of such a match occurring at random. These probability calculations are based on population statistics derived from multiple tests on multiple DNA samples. Computers help derive and maintain these statistics.

Computers also help scientists analyze DNA test results by both speeding the process and employing computational tools to augment the power of the human eye. Computer-assisted analysis of restriction fragment length polymorphism (RFLP) tests is possible using existing technology and is underway at laboratories currently involved in testing. Computerization may become more common in certain analyses of DNA amplified by polymerase chain reaction (PCR) (see chs. 2 and 3).

The law enforcement community maintains fingerprint files and books of mug shots to assist the identification of repeat offenders. If DNA tests were standardized and results computerized, they might be used in a similar fashion. Databases that would permit rapid, electronic comparison of DNA results from tests on different samples have been proposed, but they remain in the preliminary stages of development.

The possible formation of a national DNA database evokes several concerns about privacy. Because DNA is unique and so highly personal, some are reluctant to see it become part of the de facto national database. Others fear that testing will not be limited to identity but will expand to include proclivity toward disease or behavioral characteristics, which could then be incorporated in the database. Some believe it to be an inappropriate use of government authority to collect and store such sensitive, personal information. In addition, there are concerns about data security and about the quality and reliability of the information stored (8,18).

This chapter summarizes existing and developing applications of computer technology to forensic uses of DNA tests. Tools used by commercial laboratories and the Federal Bureau of Investigation (FBI) are examined, as are spinoff technologies from the Human Genome Mapping Project. The chapter also looks at technical considerations regarding widespread application of a new technology (e.g., cost-effectiveness and standardization requirements). The ability to create and secure databanks is addressed (though these issues are covered more thoroughly in previous OTA documents, see refs. 51-54), and

Box 5-A—Automated Fingerprint Identification Systems

Automated fingerprint identification systems (AFIS) have revolutionized fingerprint identification technology. A 3-minute scan of millions of prints in a master file helped police identify the man recently convicted in the California "Night Stalker" case, involving 14 homicides and at least 21 assaults. A 6-minute AFIS search, after 8 years of manual searching, led to identification of a suspect in a San Francisco murder case who pled guilty to first-degree murder after being confronted with the fingerprint evidence.

AFIS technology uses a computer to scan and digitize fingerprints, translating the unique ridge patterns and minutiae of the prints into a binary code for the computer's searching algorithm. In a matter of minutes, an AFIS computer can compare a new fingerprint with vast files of prints and make identifications that previously were possible only through a time-consuming and error-prone process of manual comparison.

This technology has greatly increased the speed and accuracy of fingerprint processing and has made it possible to conduct "cold searches" (i.e., a search where there are no suspects or other identifying information other than the crime scene prints) against very large fingerprint files. The search time in a file of about 500,000 prints ranges from a half-hour to a matter of minutes.

AFIS technology also permits the digitized fingerprint images to be stored on an optical disk and retrieved later. The current crime scene prints can be visually compared on the computer screen with retrieved images of the candidate file prints.

One AFIS computer cannot search the files of a different manufacturer's AFIS computer, but this presents only a minor problem. All one AFIS computer needs from another computer is digitized fingerprint image data to make its own search. Facsimile transmission is used to send fingerprint images from remote sites to the AFIS computer. The facsimile prints must be of high quality to substitute for the inked impressions in the AFIS, but this quality is increasingly available.

Linked photographic and telecommunications technologies are also being used to lift and transmit prints to an AFIS. The use of a remote television camera linked to telecommunications lines is under trial. A device attached to the camera converts the photographic image into digital data and sends the information via modem directly from the crime scene to an AFIS computer at the State central repository, allowing virtually instantaneous processing.

As fingerprint matching becomes a more powerful tool of criminal identification and as matching from large files becomes faster and easier, there will be increasing pressure to expand the search capability of law enforcement agencies. For instance, government employees, military personnel, and juveniles are routinely fingerprinted for reasons having nothing to do with crime. Controversy is likely to develop over whether fingerprints that were collected for noncriminal justice purposes should be included in files that can be searched by law enforcement agencies. Congress or the courts are likely to be asked to decide whether this new use violates the constitutional right to privacy.

SOURCES: Office of Technology Assessmen41990, based on Office of Technology Assessment, *Criminal Justice, New Technologies, and the constitution*, OTA-CIT-366 (Washington DC: U.S. Government Printing Office, May 1988); Bureau of Justice Assistance, *Planning for Automated Fingerprint Identification Systems (AFIS) Implementation* (Washington, DC: U.S. Department of Justice, 1988).

arguments concerning the potential usefulness and possible misuse of DNA databanks are explored.

CURRENT COMPUTER APPLICATIONS

Many crime laboratories currently use sophisticated electronic equipment to perform laboratory tasks, particularly analysis of blood for alcohol or drug content. Private and Federal laboratories engaged in DNA testing have begun to introduce computers into this new area of forensic science as well. Thus computer analysis will likely enter State and local laboratories in tandem with DNA testing procedures.

Restriction Fragment Length Polymorphism Analysis

Forensic science laboratories performing DNA tests predominantly use the RFLP methodology. Computer technology in use and under development provides tools for interpreting test results. The ultimate information to be analyzed is usually a piece of x-ray film that depicts a part of an individual's genetic code as a banding or stripe-like pattern.

Box 5-B—The Social Security Number as a National Identifier

Originally intended for use as an accounting device for contributions to the social security system, the social security number (SSN) has since been appropriated for use in maintaining the records of numerous government and private programs. Prevalent use of the SSN for non-social-security purposes raises concerns regarding its potential for misuse and abuse. It is argued, for example, that the increased use of the SSN as an identifier, coupled with rapidly advancing computer technology, has created a de facto national databank of information on each individual.

The Social Security Act (49 Stat. 620, Aug. 14, 1935) did not expressly mention the use of the SSN, but it authorized a recordkeeping scheme. Use of the SSN as a Federal Government identifier is based on Executive Order 9397 (8 FR 16095-16097; 3 CFR 1943-1943 Comp. 283-284 (1943)), issued by Franklin Roosevelt. In 1962, the Internal Revenue Service adopted the SSN as its official taxpayer identification number, and only then did its use become widespread

Citing possible harm to individual privacy through misuse of information systems, Congress established a Federal policy limiting compulsory divulgence of the SSN in the Privacy Act of 1974 (Public Law 93-579,88 Stat. 18%, codified at 5 U.S.C. 552a). This act prohibits a local, State, or Federal agency from requiring an individual's SSN as a condition of receiving services or benefits, unless the use is authorized by law. The efficacy of that prohibition is subject to question, however, Congress has subsequently not only authorized the use of the SSN, but mandated it. For instance, the 1986 Tax Reform Act requires that all children over the age of 2 claimed as dependents on tax returns have an SSN.

Currently, several public and private activities or organizations require an SSN as an identifer or authenticator, including:

. the National Crime Information Center;
. the U.S. Department of Transportation's National Driver's Register;
• driver's licensing in most States;
• educational recordkeeping, including student admissions;
. hunting or fishing licensing;
• credit checking;
• employee recordkeeping;
. obtaining a library card;
. giving blood;
.joining the Chanber of Commerce;
• enrolling in a health plan; and
. getting a telephone.

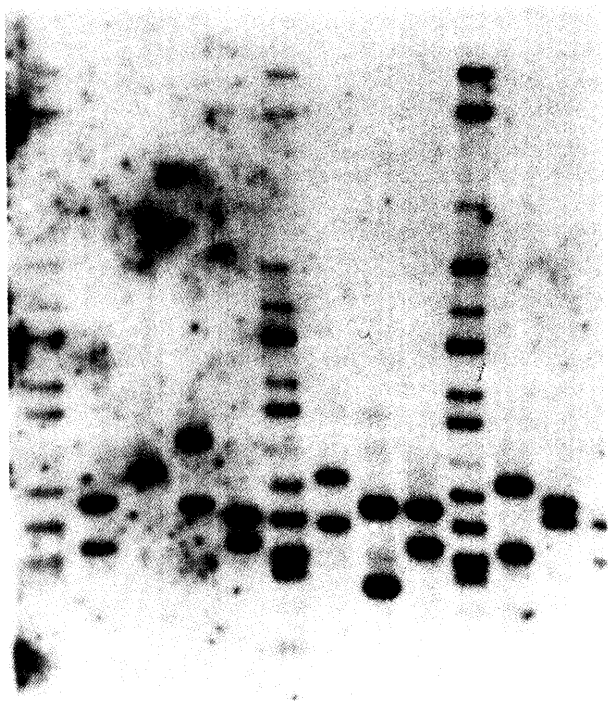
All these uses are within the law, though certainly not anticipated when the social security system was devised.

Since the SSN has become a de facto national identifier, concerns about making it tamper-proof (e.g., controlling theft or forgery of numbers) have grown. Those who seek an immutable, unique identifier may look to a numerical reduction of an individual's genetic code, such as would be contained in the FBI's proposed investigatory databases, as a replacement for the SSN.

SOURCES: Office of Technology Assessment, 1990, based on Congressional Research Service, The *Social* Security *Number: Its Historical Development and Legal Restrictions on Its Use* (Washington, DC: Library of Congress, 1985); 3. Berman and I. Goldman, *A Federal Right of Information Privacy: The Need for Reform,* Project on Communication and Information Policy Options, No. 4 (Washington, DC: Benton Foundation, 1989).

Readability of x-ray films varies from case to case. Electrophoresis as currently practiced is an imperfect process (see chs. 2 and 3). Inconsistencies in gel composition or variations in the electric field can cause a gel to "smile,'' i.e., create contortions in the lanes of DNA. Foreign matter in the DNA sample (from the restriction enzymes or the original forensic material, for instance) or impurities in the gel can diminish the distinctness of banding patterns and produce artifacts that can be misleading or misinterpreted. Over- or under-exposure of the x-ray film can decrease its legibility (figures 5-1 and 5-2). In the absence of a computer, scientists reading an x-ray film must visually estimate band location or use a ruler-two methods that are subject to fairly large discrepancies from analyst to analyst.

Figure 5-l—DNA Sizing Portrayed Through Autoradiography



An artifact from the process, the likely source of the splotches on this particular autoradiogram of one RFLP analysis, can decrease an analyst's ability to interpret test results.

SOURCE: Federal Bureau of Investigation, 1989.

Some laboratories involved with RFLP analysis use the bit pad (a digitizing tablet) to assist the scientist's eye. This computerized device requires the analyst to:

- affix the x-ray film to a back-lit tray marked with a computer-readable matrix,
- determine the position of sizing standards by locating them visually and marking their presence with a "see-through" computer mouse, and
- use the mouse to mark the location of bands in the sample and evidence specimens of DNA.

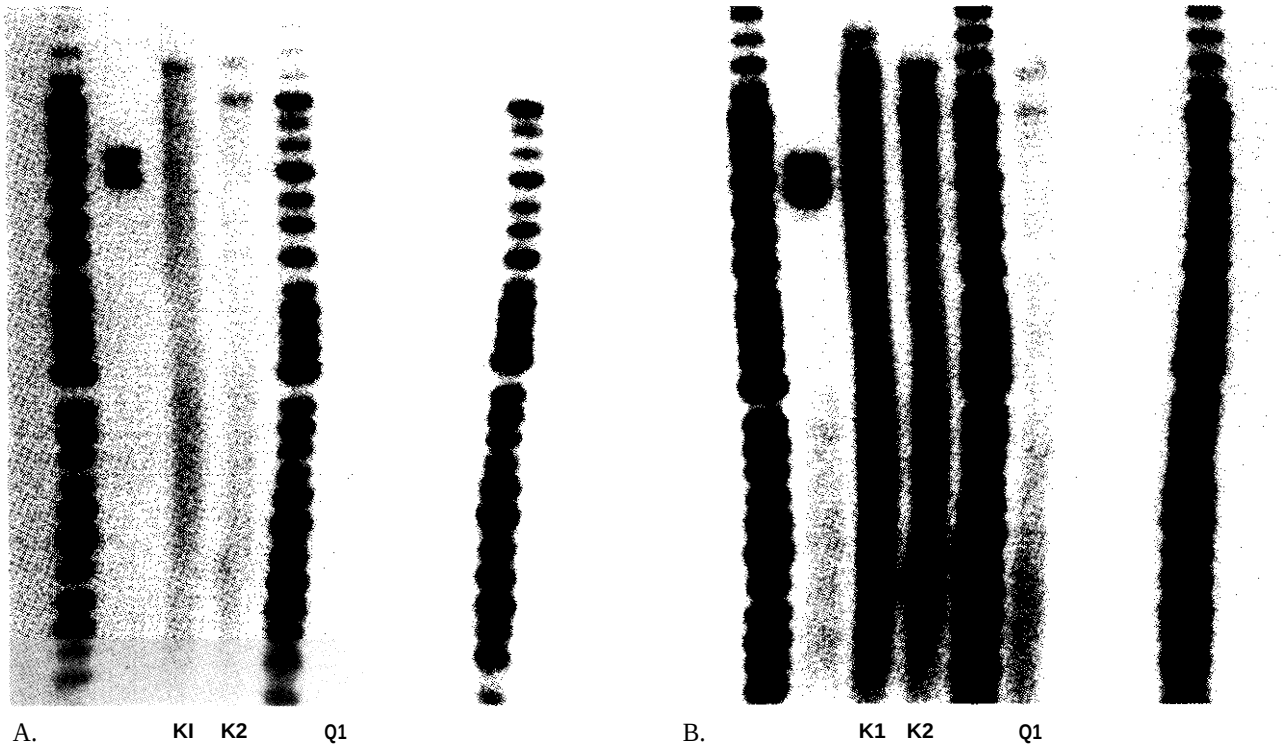
The computer calculates whether samples match, based on the analyst's use of the mouse and on quantitative matching criteria in the computer program (see ch. 3). It also derives the frequency with which that match is likely to appear in a given population, based on statistical data already present in the system. This process is repeated for each probe used on a particular specimen (5).

An alternative, somewhat more automated, aid to RFLP analysis involves application of image analysis technology. Image analysis employs a video camera to create a computer image of the x-ray film. The computer digitizes the image, i.e., divides it into small sectors, called pixels, that can be measured individually for information not easily gathered by the human eye, such as the relative density or precise relative location of bands in widely separated lanes.

Once the image is digitized, the computer can automatically mark band positions and apply a matching rule (see ch. 3) to calculate a match/nonmatch and the probability of a random match. Use of a digital image also permits application of a mathematical algorithm to straighten' the lanes, in other words, correct for migration differences across the gel. Successful application of the algorithm depends on use of DNA standards-strands of DNA that appear at known size intervals-in the testing process. If inconsistent gel composition or variations in the electric field, for instance, have caused nonuniform migration of the size markers or the specimen DNA, the computer-drawn grid linking the size markers helps the analyst estimate where a band of DNA would have appeared had the test run properly (33). In addition, software can be applied to normalize band patterns from gels run under widely varying circumstances (27). Calculation of fragment length is then based on the computer-assisted estimate (figure 5-3).

Some commercial systems can perform these functions, and the FBI has developed its own system of semiautomated analysis of the x-ray films, known as DNA autoradiograms. A description of the FBI's hardware system is available for emulation (figure 5-4), and their software system will be made available to forensic laboratories that have demonstrated proficiency in the FBI testing method. The FBI's design specifications include speed, ease of use, minimum cost, and the capacity to digitize an x-ray film, establish lane boundaries, give an integrated intensity profile, locate peaks (band position), make geometric corrections, and calculate molecular weights. Each function of the computer can be manually overridden by the operator. If the automatic features are used, it takes about 3 minutes to process an individual x-ray film, and a printout of fragment lengths or direct transfer to disk for incorporation in a database is possible (34).

Figure 5-2—Autoradiography: The Importance of X-ray Film Exposure



Over- or under-exposure of the x-ray film can also render an autoradiogram unreadable. This case involves a rape committed in the rural Northeastern United States. A semen stain (Q1) was identified on a bed sheet and was submitted to the FBI Laboratory along with blood samples from both the victim (K1) and suspect (K2). Panels A and B are autoradiograms of the same Southern blot (using one probe): Panel A is a4-day exposure; panel B a 10-day exposure. As the photographs demonstrate, results for Q1 in panel A were too weak to interpret. However, the longer exposure (panel B) provided results for Q1 that were interpretable. Once a pattern emerged, analysts determined that the suspect sample pattern matched the semen sample pattern for this particular probe.

SOURCE: Federal Bureau of Investigation, 1990.

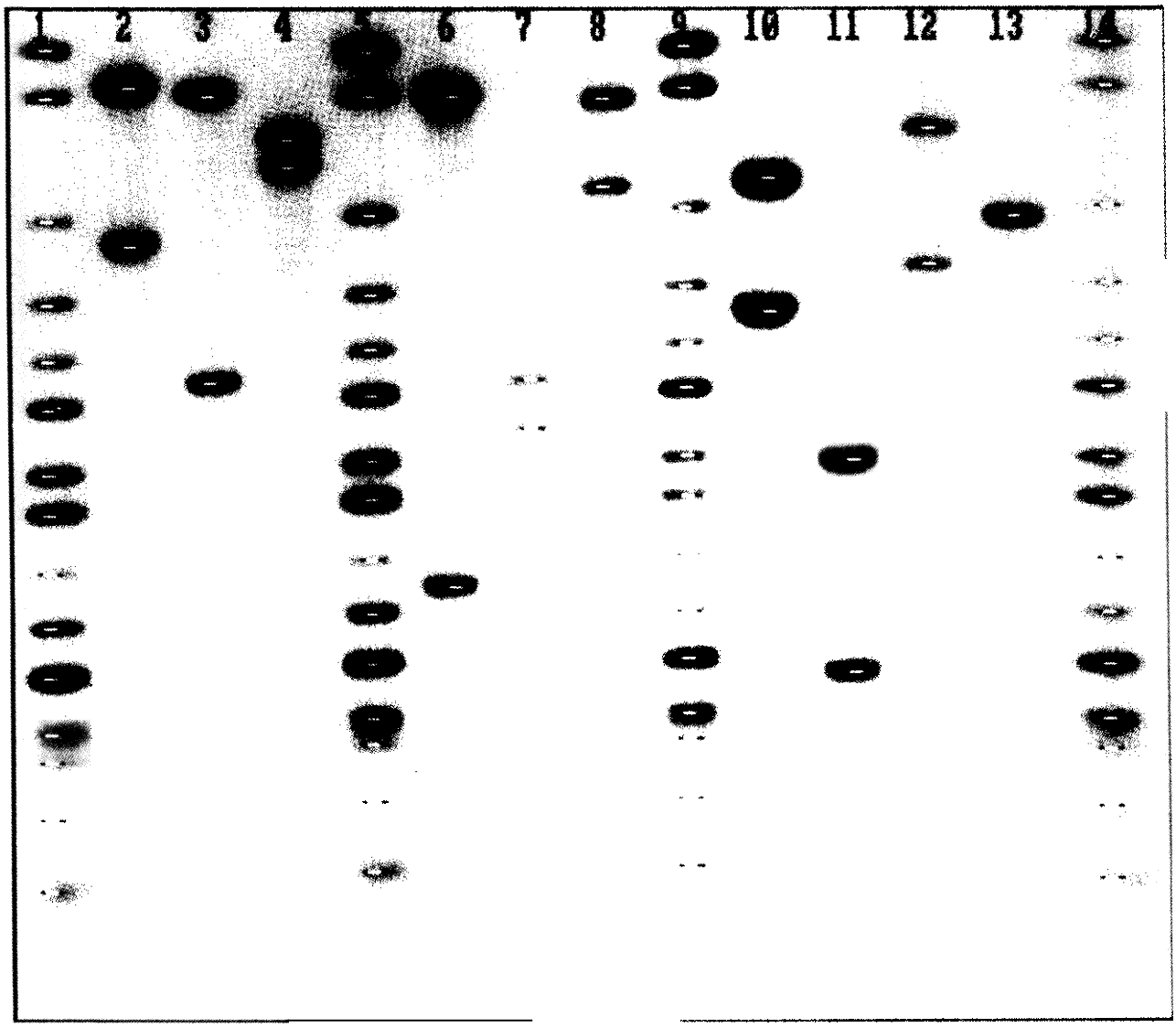
Routines for automatic location of lane boundaries, production of density profiles in lanes, and detection of band positions were originally developed at the National Institutes of Health (NIH) (43). Computers used by the Human Genome Project, financed in part by NIH, provide additional functions to improve readability. For instance, nonadjacent lanes can be juxtaposed for closer visual comparison; the computer permits only horizontal movement across the screen since vertical movement would distort band position. These computers can also produce an enhanced visual image-a printout of the digitized x-ray film-after mathematical correction (30).

Computers and Polymerase Chain Reaction

Laboratories using PCR to amplify DNA currently can test for the presence of specific alleles using a type of enzymatic ‘‘dot-blot’ method. This method involves application of a specific enzyme to a DNA sample, which will turn a specified color if the target allele is present. At least one company has considered marketing a colorimetric imaging computer to detect directly the results of enzymatic dot-blot hybridization, but such equipment is not currently in use in any commercial or government forensic science laboratories (27). In the future, DNA amplified by PCR could also be tested using RFLP methodology, and computer technology discussed in the previous section would be applicable.

Dot-blot hybridization analysis of amplified DNA yields results that readily lend themselves to databanking. Use of allele-specific probes results in “yes/no” answers-for instance, alleles 1-6 either are or are not present—that can be computerized with less interpretation (although there is some degree of subjectivity in reading the color change) than is needed in RFLP analysis, which requires

Figure 5-3-Semiautomated Analysis of DNA Autoradiogram



The lighter points within the bands of DNA on this image represent a oomputer's estimate of band positions based on its measurements of the-digitized autoradiogram. The analyst can delete-points believed to be specious or add points ignored by the computer.

SOURCE:L os Alamos National Laboratory, 1989.

calculation of fragment lengths that are distributed continuously. According to the FBI, dot-blot hybridization of PCR-amplified DNA does not yet yield certain enough identifications to warrant creation of data files (22), but the FBI plans to make provisions for recording PCR test results in its proposed investigatory databases.

Computers in Court: Cost-effectiveness

Computers make attractive analytical tools but are not yet essential or standard to interpretation of DNA tests. The amount of analyst-computer interaction varies tremendously among systems, and while the analyst may be present in court for examination

Figure 5-4-Description of the FBI's Computerized DNA Analysis System

System functions

1. Digitize autoradiograph
2. Locate lane boundaries
3. Produce integrated intensity profiles
4. Locate bands from intensity peaks
5. Do geometric correction
6. Calculate molecular weights

DNA image analysis equipment requirements

Item	*Estimated unit cost*
IBM PC/AT (or equivalent)	$4,000
Camera stand	700
Video camera	2,000
Frame buffer	2,000
19" RGB monitor	1,500
Total	$10,200

SOURCE: K.L. Monson, "Semiautomated Analysis of DNA Autoradiograms," *Crime Laboratory Digest* 15:4, *1988.*

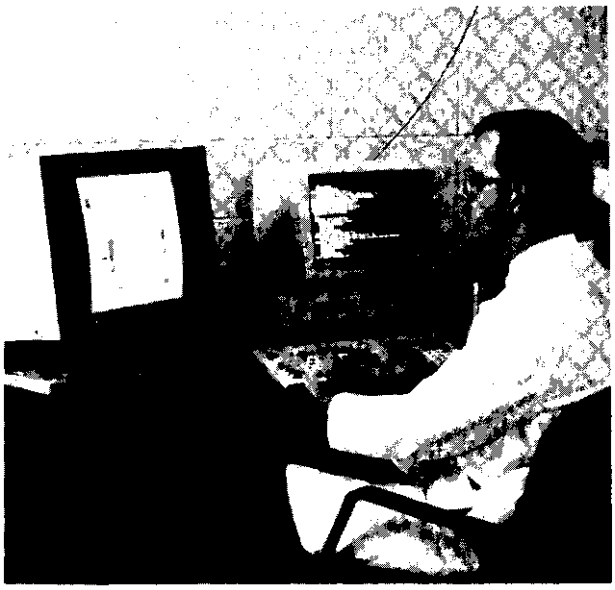


Photo credit: Federal Bureau of Investigation, Quantico, VA

The FBI DNA image analysis system and its developer, Dr. Keith L. Monson of the Forensic Science Research and Training Center, Quantico, VA.

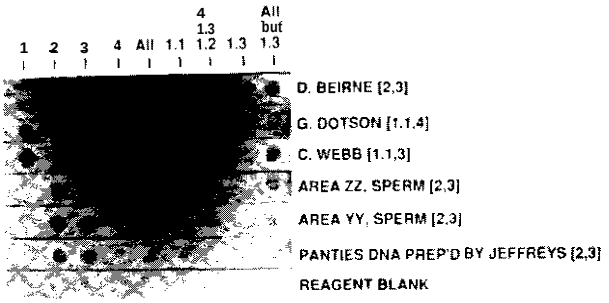


Photo *credit: Cetus Corp., Emeryville,* CA

A type of dot-blot hybridization analysis of PCR-amplified DNA was used to vacate the 1979 rape conviction in Chicago, Illinois of Gary Dotson. Dotson had been convicted of raping Cathleen Crowell Webb in 1977. Although freed on parole in 1985 after Webb recanted her court testimony, the rape conviction remained on Dotson's record. PCR amplification of forensic samples (area zz, area yy, and panties) and dot-blot hybridization at the HLA DQα-1 locus revealed that the genetic pattern of the evidence samples (type 2,3), found in approximately 5 percent of men, did not match the pattern of either Dotson (type 1.1,4) or Webb (1.1,3). Forensic analysis further revealed that a former boyfriend of Webb, D. Beirne (type 2,3), could have been the source of the semen in the evidence stains because his genetic pattern matched that of the samples. (When Mrs. Webb recanted in 1985, she said she accused Dotson to cover up sexual relations with another man.)

as a witness, the computer will not be. This raises the question, do computers lie? When an expert attests to the presence or absence of a match between evidence and suspect DNA, the court will certainly want to know if the opinion is based on computer-assisted analysis. Computers arguably locate bands and apply the matching rule (see ch. 3) more objectively and precisely than is possible with the human eye alone. Yet these capabilities also enable the computer to create a result where none was apparent before by, for instance, locating very light bands. The forensic science community may want to ensure the ability to trace analyst-computer interaction so that editing patterns can be reconstructed, and to keep the initial image available for fresh viewing by another analyst. Courts could be required to determine the admissibility of computer-enhanced images-cleaner and, arguably, more persuasive than the typical x-ray film. Faced with such decisions, courts will need assurances that the enhanced image is, in fact, an accurate representation of the test results. It will likely prove necessary to subject computer analysis tools to verification and reliability testing analogous to that received by the DNA typing technologies themselves. (See ch. 4 for a description of the admissibility of scientific evidence.)

Also, the improvements in gel analysis offered by these technologies are not without cost. Acquisition of the equipment, materials, and skills for testing already represents a major expenditure-in time and money—for forensic science laboratories. The FBI estimates the costs for its computer analysis hardware at less than $11,000 (not including software or the costs of operating a computer network) (34). Commercial systems are considerably more expen-

sive (some in excess of $100,000) (44). Forensic science laboratories typically have limited funds, and each one that undertakes DNA testing will have to determine whether additional analytical tools are necessary to meet its needs. Most of the forensic science laboratories surveyed by OTA (see ch. 6) have expressed an interest in database applications, however, and computers will be critical to the development of these capabilities.

DATABASE CONSIDERATIONS

The criminal justice community relies on specialized databases maintained by law enforcement groups, as well as on other government and private databases, in criminal investigations, sentencing, and parole decisions. Databanks of fingerprints—manually maintained but increasingly automated—provide valuable assistance in identifying and apprehending suspects. Most of the criminal justice community holds out the same hope for DNA profiles. Banks of population data will enhance the certainty of identifications based on test results and could someday be useful for investigative purposes. However, population data will be stored without reference to particular individuals so these databanks cannot be used to track suspects.

Genetic databanks are not anew idea, but their development and application to date have been limited to the medical field or research laboratories (box 5-C). Existing genetic databases provide much of the background for database proposals for forensic uses of DNA **tests.** Maintenance of genetic databases by law enforcement agencies is **a new idea with** possible positive and negative **consequences** extending beyond the **law** enforcement community.

Types of Databanks

Law enforcement proposals for DNA databanks recognize two distinct purposes for electronic storage of test results. The ability to compare greater and greater numbers of test results will enhance the legal and scientific certainty of judgments based on DNA tests. In addition, central storage of test results could ‘help officials track suspects or identify repeat offenders. Several computer files and subfiles will likely result from these various needs.

Population Statistics

The value of DNA tests for forensic science purposes lies in their unique discriminatory power. If a sufficient number of probes are used in RFLP analysis, for example, the tests cannot only exclude an individual as a suspect but can show, with near certainty, that a suspect is in fact the person represented by the biological evidence. Though subject to debate, experts have testified to the existence of a match by saying, for example, that there is less than 1 chance in 3 billion that the evidence sample came from someone other than a defendant. Since many fewer than 3 billion people have been tested, these statistics are extrapolated from smaller test pools based on allele frequencies in that population (figure 5-5). Although it is possible to extrapolate these statistics from small populations, the statistics are more credible as the number of data points (i.e., the size of the tested population) increases (see ch. 3). It would be useful, then, to combine the results of as many tests as possible to create increasingly reliable statistics, either by working with existing databanks or by establishing new ones.

Population statistics based on allele frequencies must be generated for each restriction enzyme-probe combination used in RFLP analysis. Several companies maintain proprietary databases related to their testing systems, but if their systems are not adopted by forensic scientists, their data will not be useful. The FBI has developed a database of population statistics (maintained separately for Caucasians, Blacks, Hispanics, and Asians) that will be available to crime laboratories that use the FBI DNA typing method. The database is maintained centrally by the FBI and contains technical information on DNA probes and population frequency data. It does not contain information traceable to named individuals. Rather, it records the sex and race of anonymous contributors of blood specimens. The file is used to interpret the statistical significance of DNA tests on evidence and suspect samples (20). Significant regional variations in allele frequencies will lead some jurisdictions to develop population statistics specific to their area, but the central database would be available as a check on their figures and as a source of data for other jurisdictions.

A population statistics database might someday yield information useful for additional investigative purposes. Population statistics on particu-

Box 5-C—Existing Storehouses of Genetic Information

Existing databases and repositories gather, maintain, analyze, and distribute data and materials used in genetic research that could also prove helpful to forensic uses of DNA testing. Many of the problems of information storage and networking and of sample storage and access that will confront the forensic science community are already being addressed in relation to these storehouses. Some of these resources are listed and briefly described here.

Databases

On-Line Mendelian Inheritance in Man (OMIM)-Since 1986, the Howard Hughes Medical Institute has supported computerization of this atlas of human traits that are known to be inherited As of March 1,1988,4,336 traits had been identified as genetically based, including over 2,000 diseases. The list is accessible for on-line searches free of charge.

Human Gene Mapping Library (HGML)-HGML consists of five linked database-one each for map information, relevant literature, RFLP maps, DNA probes, and contacts. All the databases are cross-referenced and linked to OMIM.

GenBank-GenBank is maintained by the Los Alamos National Laboratory and is the major U.S. database for nucleic acid sequence information from humans and other organisms. Tens of thousands of scientists now have access to the database directly or through commercial distributors.

Protein Identifiction Resource (PIR)-PIR is a resource designed **to** aid the research community in identtication and interpretation of protein sequence information. It is run by the nonprofit National Biomedical Research Foundation. Users pay a small fee for access.

Protein Data Bank (PDB)-PDB is an international computerized archive for structural data on biological macro-molecules. PDB gathers structural information critical to the understanding of how proteins function, which will lead to knowledge of the mechanisms of genetic disease and directions for drug design.

Repositories

American Type Culture Collection—This repository maintains a variety of different collections of human, animal, plant, and bacterial cell lines, hybridomas, phage, and recombinant DNA vectors. It also serves as an NIH-sponsored repository of human DNA probes and chromosome libraries, The repository also maintains a database of information on the source and characteristics of the material in its collection.

Human Genetic Mutatnt Cell Repositoty-This repository maintains a collection of well-characterizedhurnan cell cultures that are available to investigators worldwide at a nominal fee.

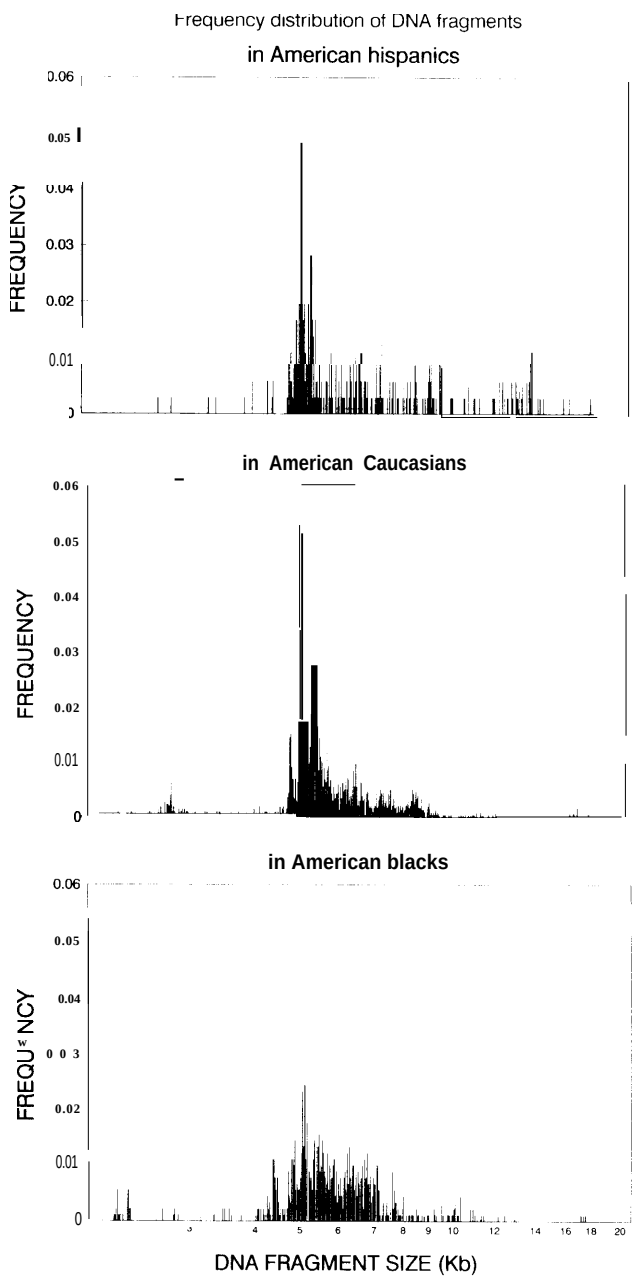
SOURCE: Office of Technology Assessment 1990.

lar alleles are currently generated by racial and ethnic classifications, since allele size and frequency can vary widely among such groups. This information could be used by police to narrow the field of potential suspects. For instance, if it is known that an allele of size "x" appears in only 0.2 percent of the U.S. Asian population, but appears in 10.0 percent of Hispanic Americans, investigators armed with test results might concentrate their efforts on Hispanic rather than Asian suspects, particularly if Asians and Hispanics are equally prevalent in the local population. However, problems such as variability y within defined population groups ("Asians" includes Chinese, Japanese, and Koreans, for instance), regional variations, and difficulty in establishing race or ethnicity (is skin color or last name controlling?) render current data insufficient to justify relying **on** population **statistics to establish the likely race or ethnicity of a perpetrator.** If law enforcement officials use this tool to develop suspects, they will also need to take measures to avoid discriminating against individuals or groups based on racial classification (e.g., using population statistics to establish probable cause).

Investigative Support Data

The law enforcement community has expressed great interest in compiling databases of convicted offenders and the results of tests performed on evidence from open cases (see ch. **6). The** FBI is currently involved in the development of a theoretical model and working prototype for an investigative DNA profiling database that would include the following types of information:

Figure 5-%--DNA Variation Among Population Groups



DNA testing laboratories report their population statistics according to racial and ethnic classifications because allele frequencies can vary substantially among, as with this probe, American Caucasians, Blacks, and Hispanics.

SOURCE: Lifecodes Corp., 1989.

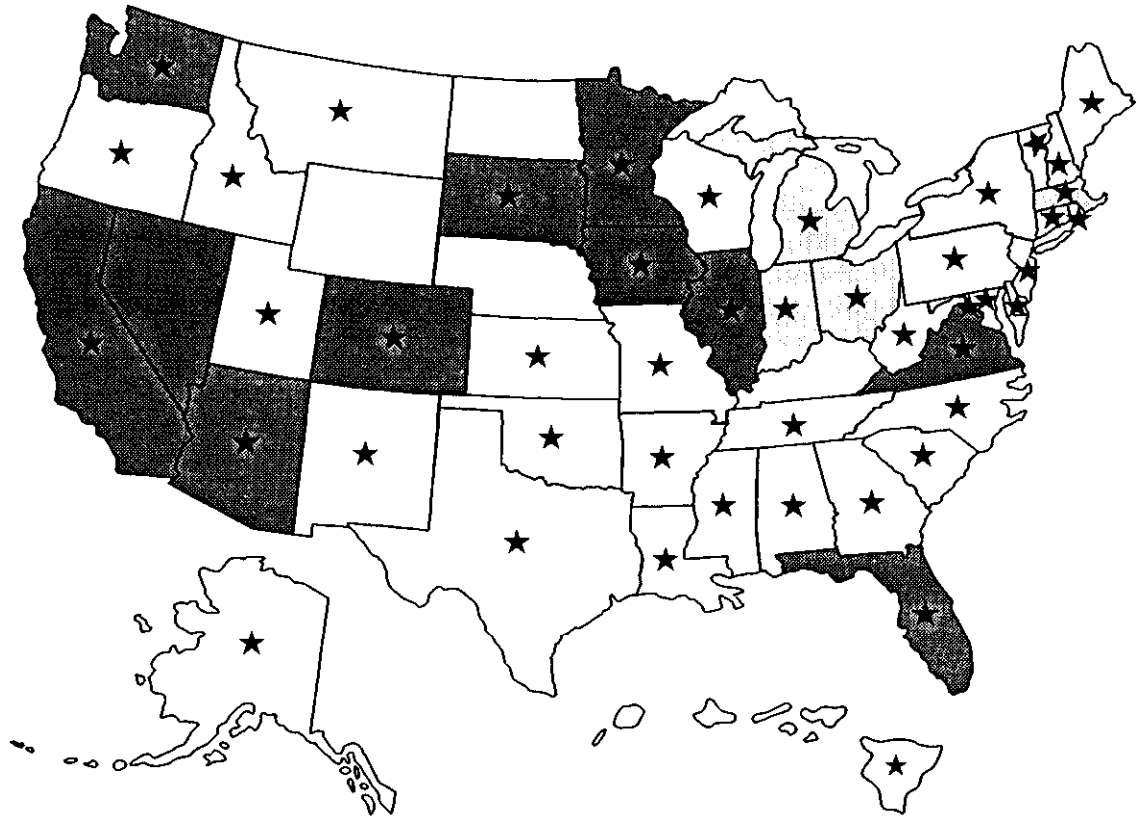
- *Open Case: The* FBI would centrally maintain a file containing DNA typing information from blood, hair, or semen evidence left at a crime scene. It would be used to help investigators in the same jurisdiction, or among different ones, determine if a series of crimes were related and committed by the same person.
- *Missing Persons/Unidentified Deceased: The* FBI would centrally maintain this file as an aid to medical examiners and investigators where other techniques, such as fingerprints, cannot be used. The FBI suggests that the file could include DNA typing information from parents who report their children missing. As children are located, the child's DNA type could be compared with parent DNA on file to effect identification.
- *Convicted Offenders: These files* would be maintained b-y the individual States according to their authority, but the FBI would provide an indexing service. It would contain DNA test results of convicted rapists, murderers, and others, much as fingerprint cards are retained. States could have access to other States' files after receiving approval (20,48).

The FBI established an advisory group to assist with database development in November 1988. The Technical Working Group on DNA Analysis Methods (TWGDAM) includes scientists from Federal, State, and local crime laboratories in the United States and Canada who are actively involved in the implementation of DNA typing. The FBI released TWGDAM'S report on development of the theoretical model for a database in October 1989 (48). States will now be selected to conduct pilot studies with the FBI prototype. After testing and modifications, the prototype can be used as a model in States' development of individual DNA profiling efforts.

State legislatures are responding to these technological developments and to law enforcement officials' enthusiasm for their potential to assist investigation. As of January 1990, at least 11 States (figure 5-6) have enacted laws to require some level of DNA typing of convicted offenders, including:

- *Arizona:* A **1989** law requires DNA testing of convicted sex offenders.
- *California: 1985* and 1989 laws require all convicted sex offenders to provide blood and saliva specimens at the time of their release from prison. Samples collected to date and

Figure 5-6-DNA Typing: Reported Uses and DNA Databank Legislation by State



● Reported use of DNA typing in that State as of January 1990 (see app. A).
Gray= Legislation proposing databanking of DNA information from certain convicted offenders.
Black=State law requires databanking of DNA information from certain convicted offenders.

First introduced in a United States criminal court case in 1986, DNA typing has since been applied in criminal investigations in at least 45 States and the District of Columbia as of January 1990. Interest in a means to store and exchange DNA test results across jurisdictional boundaries is also increasing, as reflected by State legislation.

SOURCE: Office of Technology Assessment, 1990.

future samples will be submitted for DNA testing, and the California attorney general's office has begun studies to determine the best methods for collecting and storing data.

- *Colorado:* All sexual assault offenders released on parole after May 29, 1988 will be subject to genetic testing.
- *Florida:* A 1989 law calls for a computer bank for genetic information on convicted sexual offenders.
- *Illinois: New* legislation requires those who have been convicted of sexual assault or attempted sexual assault, or who have been in an institution as a sexually dangerous person, to submit specimens of blood or saliva to the State police.
- *Iowa:* A law enacted in 1989 permits DNA testing in theriminal law context. The attorney general's office will issue rules about which crimes are covered and who will be required to provide DNA samples. Genetic profiling could become a condition of parole.
- *Minnesota:* Recent legislation requires uniform procedures for collecting DNA information in cases of criminal sexual conduct, requires that a court sentencing a person forriminal sexual conduct order a DNA analysis specimen, and provides for admission of DNA test evidence without expert testimony.
- *Nevada:* A new State law requires that convicted sex offenders submit to testing of their blood and saliva. The law also requires that the

test results be maintained in Nevada's criminal history records.

- *South Dakota:* A 1990 law allows law enforcement agencies to perform DNA typing of people convicted of sex crimes, calling for blood and saliva samples to be taken from those convicted or arrested.
- *Virginia: The* State legislature passed a bill in the 1989 session that requires DNA typing of convicted sex offenders. Virginia was the first State to establish its own DNA typing laboratory and expects to be the frost State to come on-line with a DNA databank.
- *Washington:* **State** law requires a system to collect genetic descriptions of violent and sexual offenders. In addition, King County, which includes Seattle, passed an ordinance requiring DNA testing on sex offenders.

Several other States, including Connecticut, Massachusetts, Michigan, Indiana, and Ohio have proposed DNA databanking legislation that had not yet been enacted.

Some State crime laboratories have begun to contemplate the effects of this legislation and the FBI's proposals on their operations. Virginia's laboratory believes that DNA databanking will be an extremely effective investigative tool. Staff also recognize constitutional considerations (e.g., whose test results will be included) and confidentiality requirements (16). Virginia's enthusiasm for databanking may be spurred, in part, by its success in using DNA typing to apprehend a serial murderer (12; also see box 4-B). One California crime laboratory, however, cautions that forensic science laboratories will not have the resources to examine all evidence from open cases, thus the benefits of a databank for such cases is, perhaps, being oversold (6).

Open-case and known-offenders databases could assist police in identifying suspects, but prosecutors will need to be alert to problems of overreliance on database matches. The FBI believes that the databases should be used solely as information management tools, and that ideally each sample should be reanalyzed after a suspect is apprehended (20). Reanalysis is the only sure way to link a suspect to the biological evidence in a new incident, and thus adds to the strength of the DNA evidence put before the trier-of-fact (49). Some experts also believe that reanalysis should be undertaken with a new enzyme-probe system to eliminate preelection bias (25). The proposed databases are designed to assist investigation, not prosecution, which will depend on new test results.

Technical Considerations

Successful computerization of DNA test results leaves little doubt that intra- or extra-jurisdictional databases will be possible using technologies such as those under development at the FBI and within the Human Genome Project. Usefulness of population statistics or of offender and missing persons files will be limited, however, unless standardization is pursued in testing as well as analysis. Dissimilar information cannot be compared. Therefore a successful databank will require (in the case of RFLP analysis) quality control standards for electrophoresis (e.g., gel length and composition, temperature, strength of electric charge, relative humidity), use of specific restriction enzymes, and use of specific probes in the testing process. The computer analysis must be performed according to a standardized protocol, i.e., guidelines for band identification must be established and fragment lengths must be calculated and recorded using a common numerical system. Finally, the computers used must be able to communicate.

These requirements present no insurmountable technical difficulties, but institutional protocols will be needed to establish standards and oversee quality control. Some look to the FBI for a leadership role in this area. The American Society of Crime Laboratory Directors supports the establishment of a national DNA database system based on the FBI's RFLP program (l). Others resist such a strong Federal role and suggest appointment of an independent commission for oversight of these matters. A cooperative venture between Federal, State, and local government entities and the private sector might also satisfy technical requirements. In addition to its work with TWGDAM, the FBI has convened two international symposia on forensic applications of DNA analysis to facilitate cooperation. The FBI, the American Electrophoresis Society, and the International Electrophoresis Society will cohost a similar conference in summer 1990 (44).

Peer review of results will be an important part of any database system. Users will want to be sure that the data on which they rely—whether it be for population statistics or identification-have been

carefully generated. This is likely to require that the database be in the public domain. It also could require that the database and the methodology used to create it be published and available for expert review. Particularly if the database is centralized, users will likely want to initiate review procedures and limit the ability to bypass the review procedure when adding or editing information in the system (30).

The rapid development of DNA testing technologies also leads some observers to suggest that investigatory databanks based on current testing technology would be premature. There is no consensus on how swiftly new technologies, such as PCR/dot-blot or DNA sequencing, will replace the predominant RFLP methodology, but most scientists agree that the present state-of-the-art is relatively primitive and will quickly be superseded. The FBI notes the necessity of building flexibility into any databanking system and intends to make provisions for technological developments. Yet some scientists believe that any commitment to data files based on RFLP methodology will discourage the switch to new and better testing technologies as they are proven effective, since new and old test results presumably could not be compared.

Database Management

Management of computerized DNA files will require cooperation among Federal, State, and local law enforcement agencies. Coordination of the mechanisms for information storage and retrieval will be no small task, but there is ample precedent for success.

Information Exchange

A cross-jurisdictional network will be required for a database to prove useful in detecting serial crime or repeat offenders. DNA data held in Federal, State, or local files could be exchanged through the National Law Enforcement Telecommunications System (NLETS). NLETS is a computerized message-switching network operated by a nonprofit corporation controlled by the States. NLETS does not hold or manage data files. The FBI considers NLETS a possible vehicle for DNA data transmission, but that issue has not been fully explored (1 1). The FBI appears to favor inclusion of the DNA data in a system they maintain: the National Crime Information Center (NCIC) (24).

By statute (28 U.S.C. 534), the U.S. Attorney General may acquire, collect, classify, and preserve criminal identification and crime and other records, and exchange them with authorized officials of Federal, State, and local law enforcement agencies, and with penal and other institutions; the Attorney General delegated this authority to the Director of the FBI (28 CFR 0.85). Regulations (28 CFR 20.2) permit NCIC to store identifiable descriptions; notations of arrests, detentions, indictments, and other formal criminal charges; any dispositions arising therefrom; and details of sentencing, correctional supervisions, and release (51,53,54).

In general, NCIC is used to exchange public record information among criminal justice agencies. The system includes a computer at FBI headquarters, dedicated telecommunications lines, and a network of Federal, State, and local information systems. NCIC files include information about persons who have been formally charged with criminal offenses, persons who have been formally reported as missing, and property (securities, guns, vehicles, articles, license plates, and boats) that has been formally reported as stolen. One NCIC file contains entries for persons judged to represent a potential threat to U.S. Secret Service protectees, but who have not been charged with a current criminal offense. NCIC currently contains about 20 million records (most are on property rather than people) and almost instantly answers about 75,000 inquiries a day.

The FBI has suggested that one particular NCIC file, the Interstate Identification Index (Triple I), might be an appropriate place to house DNA information (figure 5-7) (24). Triple I indexes the names and other identifiers of persons with Federal and/or State criminal history records. If a query of the index yields a result, the system indicates which jurisdiction to contact for more information. The complete records are maintained in FBI and State repositories (53).

The FBI makes decisions regarding new NCIC services with the advice of the Advisory Policy Board (APB). The APB is composed of 20 law enforcement officer members elected from the States and localities, 6 members appointed by the FBI Director (2 each from the judiciary, prosecuting agencies, and correctional institutions), and 4 members appointed by criminal justice associations (one each from the International Association of Chiefs of

Photo credit: Kevin O'Connor

J. Edgar Hoover Building, Washington, DC: Headquarters of the Federal Bureau of Investigation.

Police, the National Sheriffs' Association, the National District Attorneys' Association, and the National Probation and Parole Association) (24).

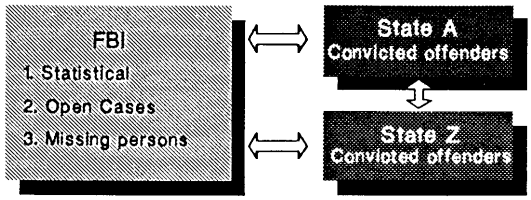
In 1987, the APB considered adding DNA characteristics to NCIC. The *NCIC 2000 Study Concept Paper* (37) proposed that DNA information be stored with other personal identtifiers and descriptive information, and also stored as part of the crime scene evidence in the modus operandi data. Inquiries containing DNA information could then be searched against those individuals having corresponding data.

The NCIC report suggested that DNA information could accompany initial entry of the person or be filed by a separate transaction, with record update capability incorporated. Data would not be provided with a routine response unless the search criteria included DNA information. A routine response not based on a DNA search would contain a statement indicating the availability of DNA information that could be obtained by use of a specific message type. DNA information would be provided as part of the validation data.

The study found that the addition of DNA information would require resources for design, development, and implementation of the storage and search mechanism; operational support; training; and technical research to develop the search algorithm. State and regional systems would also have to gear up to provide for the new transaction types and lengthy display of DNA information. The greatest drawback, however, to adding DNA information to NCIC was found to be the data-handling burden. At the time the NCIC study was drafted, no known method for automated comparison of DNA information existed, but the FBI has begun software development in this area. Starting the database from scratch was also considered a hurdle. Sensitivity and security risks associated with operation of the databank were deemed to be minimal, although obtaining suspect samples was considered somewhat troublesome. (See ch. 4 for a discussion of the Fourth and Fifth Amendment limitations on requisition of biological samples for evidentiary purposes.)

After reviewing the proposals, the APB voted in December 1987 not to add DNA information to NCIC at that time. This decision comported with

Figure 5-7—Proposed Data Files: Who Will Maintain Them?



The FBI has proposed separate responsibilities for Federal, State, and local jurisdictions in creating and maintaining DNA databanks. This effort will require significant levels of coordination and cooperation to be effective.

SOURCE: Office of Technology Assessment, 1990.

concerns expressed by a variety of groups, including civil liberties advocates and computer scientists, who believed that the proposals raised substantial privacy concerns, that the need for such information was not firmly established, and that the technology was not sufficiently developed to warrant immediate acceptance. Since the 1987 vote, however, DNA testing has spread rapidly into the criminal proceedings of many States, rekindling interest in sharing test results. Given these recent developments, the APB reconsidered its action in June 1989 and voted to endorse the FBI's plan to index and match DNA profiles in NCIC. The FBI estimates that individual State costs for implementing DNA databanking will not exceed $200,000 (11). In the TWGDAM report (48), the FBI attempts to address most of the concerns expressed by the NCIC drafters in 1987.

Fair Information Practices

Information exchanged via a DNA database would be used to assist one of the most important and sensitive government functions-law enforcement. Thus database managers in each jurisdiction will need assurances that data in the system are trustworthy and that rights of citizens are observed when data are collected and disseminated. Federal research and legislation indicate that one route to obtainin g such assurances is by adherence to fair information practices (9,53). A study released by the Advisory Committee on Automated Personal Data Systems (55) proposed a Federal "Code of Fair Information Practices" that included the following major principles:

- there must be no personal data recordkeeping system the existence of which is secret;
- there must be a way for an individual to find out what personal information is in a record and how it is used;
- there must be a way for an individual to prevent personal information that was obtained for one purpose from being used or made available for other purposes without his or her consent;
- there must be a way for an individual to correct or amend a record of identifiable information about himself or herself; and
- any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for intended use and must take precautions to prevent misuse of the data.

This Code was the model for the Privacy Act of 1974 (5 U.S.C. 552a), which relies heavily on individual initiative to ensure that records are accurate. Since the proposed DNA files could have such major consequences for both individuals and the government, the managers of these files will probably want to take special note of the fifth principle, which speaks to management's responsibility for system integrity. Sound data management principles would include security, accountability, and data accuracy and reliability (23).

Data security is critical—both access control and control of the activities of those granted access. Throughout the private and public sectors of the economy, sensitive information is entrusted to computer networks in the belief that sufficient security controls exist. Computer "hackers" regularly manage to breach these controls. High-level security measures add costs to a computer system, and a judgment regarding the sensitivity of the information in the databank will be required in order to ascertain a level of adequate, cost-effective protections (52).

Accountability controls ensure that authorized users do not misuse a system. Many systems log all entries and queries by means of user identifiers, which creates an audit trail. This technique is particularly important when sensitive information, such as criminal history, is involved.

Record quality-accuracy and reliability-is also a particular concern with criminal history records. Federal courts have imposed a duty on law enforcement agencies to maintain accurate criminal records

(28,32,47), But incidents of arrest based on false or incomplete information in NCIC continue (23). If an individual is falsely arrested based on inaccurate DNA information, there may be a cause of action against NCIC or another offending government entity.

DATABANKS AND INFORMATIONAL PRIVACY

Recordkeeping is one of mankind's oldest activities (59). Governments record births, deaths, entitlements, and penalties, for example, to help dispense the privileges and protect the rights of citizenship. Constitutional principles, particularly the right of privacy and the right to due process, establish a framework for questions about what types of records are kept, on whom, and by whom they are kept, and who gets access to them. Recognition of these rights evinces a belief that individual freedom and liberty, the foundations of U.S. society, prosper when detailed information about a person's life is private (31).

Computerized databanks raise particularly sensitive issues of informational privacy. Government and private-sector entities collect vast stores of personal information for one purpose, which, with the advent of computer networks, can easily be applied to new purposes-with or without the knowledge or consent of the data subject. The way in which this personal information is then used often has a critical impact on an individual's ability to obtain employment, credit, insurance, and other valued services and benefits. Ensuring that sensitive or stigmatizing information remains private protects an individual from harm. But regardless of the substantive harm that can be done to the victim of unfair information practices, informational privacy also safeguards the interest in personal freedom. Collecting, retaining, and disclosing personal information by institutional recordkeepers can have a chilling effect on an individual's sense of autonomy and dignity (7). Standards exist for the collection, maintenance, use, and disclosure of personal information, but they vary among jurisdictions and among data types.

What is personal information? One working definition states that it is "any information that describes a natural person, and thus is defined by the reference of the information and not by its content. Thus so long as information refers to an identifiable individual-whether that reference is made by a person's name, or a number, or some other identifying characteristic-then it is personal information' (50). Name, address, social security number, credit rating, and fingerprints are personal information; so, too, are the results of DNA tests. Personal information varies in its specficity and the degree of protection it receives. Many people share the same name, but fingerprints are unique. Addresses are usually published in the telephone book, but access to credit ratings is somewhat more restricted. Information that identifies an individual is personal regardless of content, but content determines, according to social mores, the level of privacy accorded personal information.

Governments and the private sector regularly collect and "bank" personal information, ranging from a person's birthday to whether he or she has declared bankruptcy. The law enforcement community currently maintains databases including much personal information, such as a person's name and aliases, fingerprints, criminal record, eye and hair color, and some medical information, such as whether a person has epilepsy. Law enforcement officials also have access, by statute, subpoena, or voluntary cooperation, to many other public-and private-sector databases. The Privacy Act offers some protection regarding data collection and access to information about most individuals included in Federal databases, but the act specifically provides that criminal justice agencies may exempt their record systems from many of its provisions (5 U.S.C. 552a(b)(7), (c)(3), @(2)). Regulation of non-Federal databases is left to the States, but very little privacy protection exists there. State criminal history files range from being completely open matters of public record, as in Florida, where private access is permitted, to being sealed from public scrutiny (as in Massachusetts) (51).

To secure funding, any government agency seeking to establish a new database is usually asked to demonstrate a need for the information to be collected. This exercise is intended to ensure that government funds are spent wisely and to reassure those concerned about growing data collection that a valid social purpose is being served. Many observers now ask why the FBI, for instance, needs a DNA database (14,45).

The FBI cites the fact that DNA is a unique identifier; no two people share the same genetic sequence (except for identical twins). As such, DNA can enhance the ability to identify suspects in certain types of crime-particularly rape, sometimes murder—where no other physical evidence is available. If the perpetrator is a repeat offender with DNA test results on file, identification will be complete (in the absence of error) and apprehension and prosecution eased.

Law enforcement officials often cite the high rate of recidivism among convicted offenders to justify databases. The Bureau of Justice Statistics (BJS) recently announced the results of a survey of recidivism among State prisoners released in 1983 (10). The report showed that 62.5 percent of this group had been rearrested within 3 years, with 41.4 percent returning to prison. The rate of rearrest among violent offenders was 59.6 percent. Released rapists were 10.5 times more likely to be rearrested for rape than other released offenders, and released murderers were about 5 times more likely than other released offenders to be rearrested for homicide. The study also revealed that one out of every eight rearrests was for a crime committed in a different State from where the prior offense occurred. The FBI believes that DNA databases might significantly aid their efforts to solve the high number of forcible rapes (92,486 reported in 1988) and of murders and non-negligent manslaughter cases (20,675 reported in 1988) in this country, as well as a growing number of serial crimes (21).

Those less inclined to increase the amount of personal information stored in government databases could cite other aspects of the BJS study. For instance, only 6.6 percent of released murderers were rearrested for homicide and only 7.7 percent of released rapists were rearrested for rape (10). Some cite the fact that many accused rapists choose to litigate only the issue of consent, thus the source of the biological evidence—the only issue that can be addressed by DNA testing-is never in question (8). Other research shows that blood was available to link a suspect to murder in only 15 percent of cases, semen available to link a suspect to rape in 10 percent of cases, and hair available to associate a suspect to the crime in murder or rape cases only 5 percent of the time (41). These statistics make a less compelling case for a database than those presented by database advocates and suggest a need to weigh the social benefits of investigatory databases against the potential social costs.

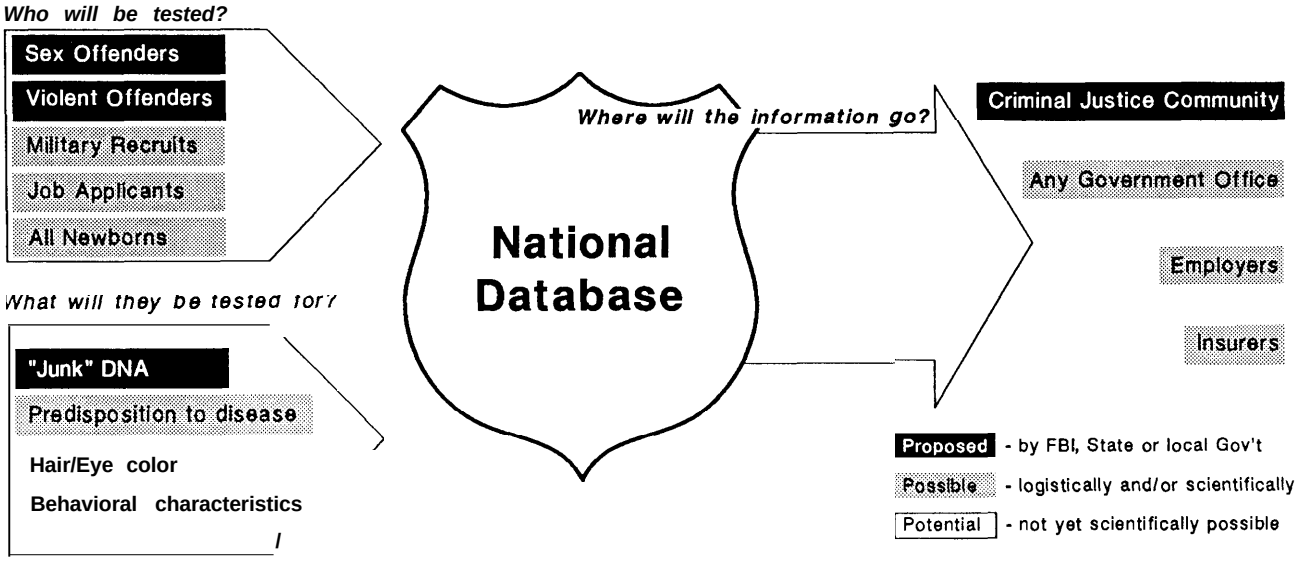
New means to detect and deter crime generally compel great respect in this country. When a social goal, such as crime control, competes with a fundamental right, such as privacy, however, it is not a foregone conclusion that the social goal will prevail; relative weights must be established in each case (29). The effort to balance law enforcement's advocacy with counter arguments from database opponents requires a determination of the individual liberties that might be compromised by the databases (9,19,42). A number of questions about where the collection of such data might lead must be posed and analyzed.

Who Will Be Tested?

Law enforcement proposals to date generally would limit test populations to violent offenders, or to the even smaller population of sex offenders. Law enforcement databases currently record much personal information, of varying sensitivity, on all offenders (figure 5-8). Some commentators view DNA information as no greater an infringement on privacy than anything currently collected. Others find DNA data increase the sensitivity of the criminal history records to unacceptable levels. These experts tend to view criminal records as a civil disability imposed in addition to the criminal penalty. A civil disability is any forfeiture of right or privilege exacted by society that hinders a person's ability to function normally after completing a criminal sentence (e.g., loss of voting rights). If adding DNA information to criminal records further discourages a decision to hire an ex-felon (e.g., because it revealed potential for a serious and costly health problem), that would bean imposition of civil disability and a potential threat to rehabilitation that should be considered (26). Imposition of a greater civil disability may or may not be a price society is willing to pay for the benefit DNA records provide.

Once violent-offender databases were established, would justification for testing all convicted offenders be found? No specific proposals for such testing have been made, but OTA's survey of State and local crime laboratories (see ch. 6) found that many labs are considering applying DNA tests in cases of suspected homicide, sexual assault, violent crime, serial crimes, hit and run, and robbery when crime scene evidence is available for comparison. Criteria

Figure 5-8—How a Database of DNA Information Could Be Created and Used



The law enforcement community cites a need for a DNA database to apprehend repeat offenders and solve serial crimes; the military for additional identification (e.g., for victims of wars and mass disasters). Civil liberties experts, however, fear that DNA testing could expand beyond legitimate identification needs, and that test results would be widely available through the de facto national database.

SOURCE: Office of Technology Assessment, 1990.

for establishing the types of crimes suitable for DNA testing include considerations of costs, whether conventional methods are adequate, and any FBI guidelines that are established. Even if test results are produced in a wide variety of crimes, they need not all be included in investigatory data files, but could be.

Proposals to establish DNA databases for identification purposes do not stop with law enforcement. The military services are considering proposals to begin using DNA tests for criminal justice purposes, and are also contemplating performing DNA tests on all current personnel and military recruits to establish a database that would enhance the ability to identify those killed in wars or the victims of mass disasters (57,58). Cases like that of Cpl. Carl Houston, whose body was identified 43 years after he disappeared, might be resolved more quickly and reliably if a DNA database existed. So, too, might situations like the Gander air crash in Newfoundland, Canada, where noncomputerized dental records were destroyed in the disaster (46). (Normally records on military personnel are transported separately from the individuals to which they refer; in the Gander incident, however, troops returning from the Sinai were accompanied by their records, so identification of victims from the plane crash following refueling in Newfoundland was more difficult.) But this database might also be a permanent computer record of personal information on all military personnel. Will society consider that an appropriate use of personal information?

Should parents be able or compelled to store a DNA print of their child for use in the event of a kidnapping or to resolve allegations of switched babies? Such a step might ensure the existence of an immutable identifier, readily and scientifically attributable to an individual, unlike an assigned social security number, for instance (box 5-D). On the other hand, it might also encourage genetic discrimination if DNA samples were probed in-depth. In the mid-1960s, scientists found a high incidence of the XYY chromosome pattern in violent criminals. The press and the public, including some scientists, called for prenatal screening or newborn testing so that those genetically predestined to a life of crime could be tracked. Some innocent children were branded as inferior before this theory was discredited (15).

The Twigg case (4) also raises interesting points on this issue. The Twiggs' daughter, Arlena, suffered from a heart problem, and genetic tests performed before her death revealed that Arlena was

Box 5-D—Newborn DNA Typing

Parents sometimes lose their children-they are kidnapped or switched; they run away. If the child and parents are separated for **a period** of time that renders normal, physical identification difficult or unreliable, DNA testing **can** assist reunification. Paternity, or parentage, testing is a frequent application of DNA typing, and well within the capabilities of current DNA technologies.

If, however, one or both parents is unavailable at the time the child is recovered, or if there is no clue to connect a child with his or her parents, accurate identification becomes more difficult. That problem has led some experts to suggest that children should acquire a DNA profile at birth, which could be stored for direct comparison with a profile taken at the time of recovery. One company recently began marketing such a service.

Lifebank, Inc., a subsidiary of Quantum Chemical Corp. and sister company of Lifecodes, was incorporated in July 1989 for the purpose of providing neonatal DNA storage services. Lifebank will extract DNA from a newborn's umbilical cord blood and create a DNA profile using Lifecodes' technology. The profile and remaining DNA sample will be preserved at Lifebank facilities for 18 years.

According to Lifebank, the DNA information will be maintained with strict confidentiality. Only a child's parent or guardian will have access to the information; access will be controlled through a passbook/code number system. The company foresees using the DNA profile only for identification purposes, e.g., to reunite parents and missing children. The company does not intend to make the umbilical cord blood available for paternity testing or further genetic testing.

Lifebank began marketing their services in December 1989 through pediatricians and obstetrician-gynecologists. It hopes eventually to expand its market, perhaps by providing DNA banking services for the military or complete families.

SOURCE: **Office of** Technology **Assessment,** 1990, based onL. Kelly, **Lifebank,** Inc., **Bridgewater,** NJ, personal **communication,** January 1990.

unrelated to either parent. The Twiggs, seeking to learn what happened to their biological daughter, requested a judge to compel genetic testing on a child, Kimberly Mays, who was born at the same time and in the same hospital as Arlena, but who was raised by another family. Kimberly's father, Robert Mays, resisted this request, as he believed it would

Photo credit: National Center for Missing and Exploited Children, Arlington, VA

Some propose that DNA prints stored in a databank could be useful in missing children investigations.

unnecessarily disrupt his child's life. In 1989, the Twiggs and Mr. Mays compromised: the Twiggs agreed not to seek custody in return for Mr. Mays agreeing to the tests. Eight genetic tests performed at Johns Hopkins University confined that Kimberly is the Twiggs' biological child. If a judge approves the agreement between the Twiggs and Mr. Mays, the Twiggs intend to seek visitation rights. The Twiggs have sued the hospital where the girls were born, charging negligence, malpractice, or deliberate acts. Existence of a DNA databank might preclude the need for court intervention at the testing stage in similar cases (each child's DNA test results would be on file), but it would do little to resolve the social or moral dilemmas involved.

Would an adult be permitted to have a childhood DNA record purged from a databank, or control how that record was used? Satisfactory answers to these questions may require answers to additional, broader questions.

What Do the Tests Reveal?

Forensic RFLP probes in use and under immediate development identify highly variable, noncoding segments of the genome-sometimes called 'junk' DNA—that reveal only an individual's identity. DNA profiles in this respect resemble fingerprints—they are unique, but otherwise uninformative. On the other hand, the *DQx* enzyme system used to test

PCR-amplifed DNA can reveal important information regarding a disease condition (see ch. 3).

For most people, the information most likely (at this time) to be added to a criminal history record—RFLP results—probably would not escalate privacy concerns associated with those files because scientists cannot yet make disease associations with the type of information now being collected. Similarly, individuals are asked to provide personal information, from social security number to health status, for so many purposes, that files of "junk" DNA information on military recruits or newborns might be found unobjectionable.

Some are more cautious about DNA collection and storage. They include genetic data in that category of information-along with religion, votes, special confidences-that civil liberties tradition in this country protects from compelled disclosure. These observers are particularly wary of forensic science laboratories applying probes used for medical diagnosis.

DNA testing methods applicable to forensic science are the same as those used in medical diagnostics-to reveal sickle cell or Huntington's disease, for instance. Evidence of disease is personal information and normally designated as highly sensitive. If it were added to a criminal history file, any civil disability created by the file might be compounded, particularly if the information were available to prospective employers. Society might be willing to impose that disability on crimainals, but would likely be more hesitant with regard to children or military personnel.

Diagnostic tests do not reveal unique identity in the reamer of 'junk' DNA, thus no suggestion has been made to include DNA-based medical information in law enforcement or other identification databases. However, some probes used in forensic science locate alleles that lie near a disease locus, thus there may be some association between the "junk" DNA and the disease locus. The possibility exists to test DNA acquired specifically for identification purposes for disease information and to include that information in a database. This option may become more attractive over time, especially as the number and types of probes for genetic disorders increase.

Some scientists developing the DNA tests believe it will be possible to identify behavioral and other mental characteristics within a decade (e.g., genetic bases for schizophrenia and bipolar disorder have been hypothesized). Many forensic scientists do not believe a legitimate law enforcement purpose could be established for such tests and, thus, do not advocate their use in the criminal justice community. Such tests are not yet available, but the civil disabilities attached to misuse of such information, if the tests are developed, could be enormous.

Obviously, testing technologies are under rapid development, with new probes becoming available regularly. Database proponents have recognized the need to build flexibility into any system adopted to accommodate new developments. Still, a problem with the long-term value of the database will arise unless provisions are made to update test results as new testing methods become available. This dilemma leads to another broad and unresolved question.

How Will DNA Information Be Stored?

Complete genetic information on an individual resides in the DNA sample acquired for testing. Tests render portions of this basic information accessible, but are limited in scope, i.e., one test can only reveal so much about an individual's genetic makeup. Current technology permits several different probes to be used on one Southern blot, but each one has a limited lifetime and a limited amount of information on it. DNA itself can be frozen without significant degradation, and technologies exist to identify the small mutations that can occur during storage (39). Thus three levels of data storage will be available to database managers: test results, Southern blots, and a DNA sample.

Crime scene evidence and DNA samples from victims and suspects are being and will continue to be tested to help identify perpetrators. Current proposals for law enforcement databases anticipate a need only for test results of convicted offenders and unidentified crime scene evidence in investigatory databanks, which, since tests are currently limited to identification, limits the privacy concerns associated with those databanks. To further avoid privacy concerns, law enforcement officials could take specific steps to assure that test results and test materials of victims (and of suspects who are not convicted) are destroyed. Consider, though, a recent

English case. T'he defendant voluntarily contributed a blood sample during a criminal investigation and was eliminated as a suspect in that case. Police retained the test results, however, and compared them with evidence from other cases, leading to the individual's arrest on another rape charge (17).

A Federal court has determined that NCIC'S authorizing statute (28 U.S.C. 534) only permits storage of information on individuals who axe subject to formal criminal proceedings, thus it may be illegal for NCIC to maintain victim DNA information in any form traceable to the individual (32). The databanks of population statistics may include the results of tests run on both victims and suspects, but since these data are maintained anonymously, privacy concerns again are limited.

Although many officials favor some means of storing test results, no consensus exists within the forensic science community on the issue of DNA sample storage. Two panels convened to help formulate policy in this area reached slightly different conclusions. The New York State Forensic DNA Analysis Panel recommended that DNA samples not be stored in order to avoid improper use (38). The Ad Hoc Committee on Individual Identification by DNA Analysis of the American Society of Human Genetics (ASHG) concluded that it would be appropriate to retain DNA samples if permissible uses were defined and adequate rules of access and disclosure implemented (3).

The main reason to store a DNA sample would be to facilitate retesting whenever necessary to keep up with changes in preferred testing technology or information requirements. Standardization of identity tests would eliminate the need for retesting unless new technologies were adopted or officials determined a need for additional genetic information. If retesting is required, it might also be possible to obtain new samples from convicted offenders, making storage unnecessary. Obtaining a DNA sample from an involuntary donor for purposes unrelated to a specific crime is likely to be problematic, however.

Many ethicists believe sample storage is inappropriate, primarily because it increases the likelihood that specimen DNA will be tested for information beyond unique identity. Since noncoding sections of the genome vary most between individuals, probes for "junk" DNA, rather than medical diagnostic probes, will likely continue to be applied to establish links between a suspect and a crime scene. If a suspect's sample is available for further testing, however, the opportunity arises for use of medical diagnostic probes, which would generally be considered a misapplication of the technology. Destruction of samples, except for crime scene evidence, and maintenance of only 'junk' DNA test results would resolve this issue. Again, privacy concerns are especially acute with regard to storing samples from victims and unconvicted suspects, and some suggest that the law enforcement community take special steps to assure that these samples are destroyed.

If sample storage is deemed necessary for forensic applications, forensic scientists and law enforcement officials could turn to work done by the Ad Hoc Committee on DNA Technology of the ASHG. This group has published some "Points to Consider" regarding preservation of DNA samples taken for diagnostic purposes (2). The guidelines address questions of ownership, confidentiality, release to third parties, quality assurance, and certification.

Southern blots, a middle ground, can be stored and reprobed, but contain a limited amount of information. The limit is imposed by the life of the Southern blot, which can be reused only so many times, and by the restriction enzyme used to fragment the DNA, which limits the probes that can be used. In some circumstances, Southern blot storage could be necessary to preserve the evidence. Otherwise, this storage mechanism offers few technical benefits and potentially raises many of the same privacy concerns associated with sample storage.

Legislatures appear to be wary of imposing substantive restrictions on collection or storage of personal information (7). Most legislation focuses on controlling access to information already collected. The Supreme Court, too, has seemed willing to defer to a government's perceived need for personal information if proper access controls are employed (60). Thus another question regarding a potential DNA database is raised.

Who Will Have Access to DNA Information?

Civil liberties tradition holds that sensitive information collected under government authority should not be shared indiscriminately. Noncriminal justice use of NCIC'S Triple I file is prohibited (53), thus access to information in that index is quite limited.

However, FBI proposals for DNA databases envision maintenance of DNA information in State criminal history files, which vary in their accessibility. Concerns about some types of criminal behavior (particularly sex offenses) have led Congress to require that State criminal history files be opened to certain noncriminal justice agencies and employers. For example, in 1984 Congress required States to establish procedures to provide for nationwide criminal history checks for all operators and employees of child-care facilities (Public Law 98-473). There has also been growing interest in implementing criminal record checks for teachers, youth group leaders, and elder-care providers. In addition, there has been increased emphasis on criminal history record checks for current and prospective Federal employees (53). In a majority of States, private organizations can lawfully obtain conviction information (and often arrest information) from State criminal history record files, though conditions regarding access range from very strict (e.g., in Massachusetts) to quite liberal (e.g., in Florida).

The Supreme Court recognizes a strong privacy interest in criminal history records (56). The Supreme Court has ruled, however, that criminal justice agencies are not required to maintain confi dentiality of official records (40). The Privacy Act permits the Attorney General to exempt the FBI from its provisions, but the FBI has adopted privacy regulations for governing NCIC (28 CFR 20). States that violate privacy standards with regard to access to FBI files can be denied NCIC services, but compliance is largely voluntary since the FBI has no active enforcement process (51).

Regulation of access to files maintained by private laboratories remains an open question. Files created for criminal justice purposes may be subject to Federal or State legislation. New means of access control may be necessary if private DNA databases are established to help, for instance, parents identify their children.

Investigatory Use of Population Statistics

The preceding questions have dealt mainly with the possible informational privacy implications of investigative support databases such as those proposed by the FBI. Databases of population statistics, which do not contain information traceable to an individual, could also change the nature of law enforcement in the United States. Consider the following scenario: A rape occurs in a small community with a population equally divided between Blacks and Caucasians. Semen recovered from a vaginal swab expresses allele size characteristic of 9 percent of the Black population and 0.5 percent of the Caucasian population. No other evidence is available. The scenario raises the following questions:

- Does the entire Black male population in the community become suspect?
- Are the statistics sufficient to issue a warrant demanding blood samples from all Black males in the community?
- If a warrant could not be issued, would a general call for "voluntary' testing of Blacks be condoned? (Box 5-E describes a case involving voluntary testing.) Would failure to volunteer create probable cause for a warrant to be issued?

A Supreme Court case from 1969, Davis v. *Mississippi* (13), involving fingerprint evidence raised similar questions. In *Davis*, **a** rape victim described her assailant as a young, Black man, but could not identify him. Police recovered partial fingerprints from a windowsill. Over a 10-day period following the rape, police, without warrants, questioned and fingerprinted at least 24 Black youths and interrogated 40 to 50 others. Police eventually arrested, based on fingerprint evidence obtained during warrantless questioning, a youth who had done yardwork for the victim. The Supreme Court characterized police behavior in *Davis as* **a** dragnet and excluded the fingerprint evidence as obtained in violation of Fourth Amendment protections. The majority of the court refused to accept the State's argument that the inherent reliability of the fingerprinting process would exempt it from probable cause requirements.

The facts of *Davis* and the Pitchfork case (box 5-E) indicate that powerful identification tools can tempt police to extend their investigatory actions beyond generally accepted bounds. Observers have recognized the power of new technologies to trigger dragnets and searches where there is no specific evidence of wrongdoing. This power effectively shifts the presumption of innocence to one of guilt, with the burden of proof on the targets of the investigation (31). One State attorney general has noted the possibility that DNA typing technologies in particular may create a temptation to engage in

Box 5-E—The Leicester Case: DNA's Criminal Debut

On November 21,1983, Lynda Mann, 15 years old, was sexually assaulted and killed on an isolated footpath in the small English county of Leicestershire. Semen recovered from an internal labial swab and a deep vaginal swab was tested. The blood tests could not positively identify the killer, and the scientific label 'Group A secretor, PGM l+," a blood type shared by just 10 percent of the population, was the only clue police had.

The police went to every residence in three nearby villages filling out a pro forma document on male residents between the ages of 13 and 34 (an arbitrary range). Patient records from the local psychiatric hospital were also carefully examined. The local newspaper published appeals for help, leading to many tips, all of which proved useless. The investigation team started out with 150 officers, dropped to 8 by May, and was disbanded in August 1984. One-hundred-and-fifty blood tests on potential suspects were performed with no positive results.

In a neighboring village, 15-year-old Dawn Ashworth was similarly slain on July 31, 1986. Police assumed this was a serial murder, and semen was recovered from a vaginal swab and a clothing stain.

On August 8, 1986, police arrested 17-year-old Richard Buckland, a kitchen porter from the psychiatric hospital, for Ashworth's murder. Buckland had a history of sexual behavior that would fit the pattern presumed for the murderer and had known the victim. After prolonged questioning, he made a graphic confession to killing Ashworth.

At this point, the police officer charged with investigating Mann's murder decided to try to connect Buckland to her death. He delivered the semen samples taken from Mann and Ashworth and blood from Buckland to Dr. Alec Jeffreys at Leicester University. Jeffreys, well known because of a highly publicized immigration case in which he applied his new technique of "DNA fingerprinting," accepted the request for assistance. He concluded that both girls were raped by the same man, and that Buckland was *not the* perpetrator. On November 21, 1986, Buckland became the first accused murderer in the world to be set free as a result of a DNA test.

A new inquiry to investigate both murders began immediately, and on January 2, 1987, police announced a "revolutionary step"—a campaign of voluntary blood testing for every male resident in the three villages. Men were requested by form letter to appear at a certain time for sampling. Collected blood and saliva was first tested for PGM 1+, A secretor characteristics; any blood meeting these criteria was forwarded to Jeffreys for the DNA test. The Police made "house calls" on those men who failed to appear. English civil liberties experts expressed concerns about coercion and the ultimate disposition of test results.

Colin Pitchfork received his notice to appear that January and told his wife he was afraid to give blood because of his criminal record for flashing. Pitchfork eventually convinced a coworker, Ian Kelly, to give under Pitchfork's name using a falsified identity card, and Pitchfork received notification of a negative test.

By May 1987, the police had taken samples from 3,653 men and boys, a 98 percent response rate, but had not found the killer. In August, Kelly admitted his act of deception to other coworkers, one of whom had also been approached by Pitchfork. Six weeks later the police were informed and Kelly was arrested. Pitchfork confessed to both murders on his subsequent arrest in September 1987.

Pitchfork received a double life sentence for the murders, a 10-year sentence for each of the rapes, 3 years each for two earlier sexual assaults, and 3 years for conspiracy, all to be served concurrently. The concurrent sentences mean he could be released within 10 to 12 years. At sentencing, the judge noted that without DNA testing, Pitchfork might still beat large.

SOURCE: J. Wambaugh, *The Blooding* (New York, NY: William Morrow& Co., Inc., 1989).

genetic ''fishing expeditions.' A professor of forensic science has voiced a concern that mirrors the third query in the hypothetical case, i.e., calls for massive voluntary DNA testing to solve a crime will make a suspect of everyone refusing the test (35). Existing interpretations of Fourth and Fifth Amendment protections may also control application of DNA typing technology, but the issues cannot be ignored as the technology becomes more accessible.

To date, few population statistics have been published, and these have received minimal scrutiny. Thus it maybe unlikely that police will depend on them to help direct their investigations, especially since many scientists believe that population statistics will never be sufficient to indicate reliably a perpetrator's race (36). Their very inadequacy, however, heightens concern that limits to the technology be recognized prior to reliance.

FINDINGS AND SUMMARY

Enthusiasm for and availability of DNA typing technologies among the forensic science community grows daily. Concerns about the ability to share information collected from these tests directly follow cost and court acceptance as priority considerations. Several States are debating funding the acquisition of the testing technologies and/or ordering study of networking DNA results. Despite the rapid pace of introduction, the relative newness of the technology provides an opportunity to consider the pros and cons of databanking before making major investments.

The technical capability to network DNA information exists, but should it be used? Beyond the necessity for population statistics, the main rationale for databanking test results appears to be the desire of law enforcement agencies to catch repeat offenders and to aid investigation of serial crime. Experts point to recidivism among rapists as an illustration of a databank's usefulness-recidivists would be more quickly identified if prior test results were on file. Some experts also believe that serial crime could be far more prevalent than realized. A database permitting jurisdictions to store DNA information from unsolved crimes could enhance the ability to identify crime as serial in nature, and therefore encourage collaborative endeavors to solve such crimes.

On the other hand, collection of "junk" DNA (noncoding segments of the genome) for identification purposes will, according to some experts, start society down the slippery slope to unwarranted invasion of privacy. These experts fear that suspect samples will be tested for medical information or behavioral characteristics, and that information generally accorded privacy protections could be entered into computer files that normally are not considered sensitive.

Some experts also suggest ''technology-forcing' type reasons to delay databanking at this time. They believe that current tests are primitive but that technology is rapidly advancing. If extensive databasing is done using current, less sophisticated tests, there may be reluctance to adopt new and better technologies that could detract from the usefulness of the initial databases. Of course, this problem would be diminished by a decision to store DNA samples in addition to test results. The database could be constantly updated by performing the newest tests on stored specimens. Such a procedure, however, might increase the likelihood that specimens would be tested for information other than "junk" DNA as new probes are developed, which raises civil liberties concerns.

Databanks of population statistics will likely grow with or without forensic science test results (e.g., through efforts to map or sequence the genome). Since these data do not identify individuals, misuse could only occur in investigations where no suspect has been identified (e.g., to focus efforts unfairly on a particular racial or ethnic group). Such broad applicability of the technology means that possible misuse in forensic science would have to be controlled by limiting access to the population statistics, rather than by deciding not to bank the information.

If deliberation on the pros and cons of databanking are resolved in favor of its use, some technical concerns must be addressed. Successful networking will require databases built around test results derived from standardized procedures and analyzed according to standardized protocols, to be conveyed on standardized computer hardware and software. At the moment, no institutional framework exists to require such standardization, but it appears to be in the best interests of both the States and the FBI. Various means to ensure data integrity-both through peer review and security measures-also need to be integrated in any computer system.

CHAPTER 5 REFERENCES

1. American Society of Crime Laboratory Directors, "Policy Statement on Forensic Applications of DNA Typing, ' adopted by the Board of Directors, May 3, 1989.
2. American Society of Human Genetics, Ad Hoc Committee on DNA Technology, "DNA Banking and DNA Analysis: Points to Consider," *American Journal of Human Genetics 12:5, 1988.*
3. American Society of Human Genetics, Ad Hoc Committee on Individual Identification by DNA Analysis, ''Individual Identification by DNA Analysis: Points to Consider, ' *American Journal of Human Genetics 46:631-634, 1990.*
4. *Associated Press*, "Lawyer for Twiggs Says Robert Mays Could Be Scaring Girl in Custody Case," Wauchula, FL, Jan. 2, 1989; "Genetic Tests Confirm Florida Baby Swap," Clearwater, FL, Nov. 19,1989.
5. Balazs, I., Lifecodes Corp., Valhalla, NY, personal communication, April 1989.

6. Bashinski, J.S., Oakland Police Department, Criminalistics Lab, personal communication, April 1989.
7. Belair, R.R., "Information Privacy: A Legal and Policy Analysis," *InformationReports and Bibliographies 12:2, 1983.*
8. Bereano, P.L., Professor, Engineering and Social Policy, University of Washington, testimony before U.S. House of Representatives, Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, Mar. 22, 1989.
9. Berman, J., and Goldman, J., *A Federal Right of Information Privacy: The Need for Reform,* Project on Communication and Information Policy Options, No. 4 (Washington, DC: Benton Foundation, 1989).
10. Bureau of Justice Statistics, *A Survey of Recidivism Among Prisoners Released in 1983* (Washington, DC: U.S. Department of Justice, March 1989).
11. Castonguay, R.T., Federal Bureau of Investigation, Washington, DC, personal communication, April 1989.
12. Dabbs, D., "The Use of DNA Profiling in Linking Serial Murders," *Medico-Legal Bulletin 37:6, 1988.*
13. *Davis v. Mississippi, 394* U.S. 721 (1969).
14. Edwards, D., "Chairman's Opening Statement," U.S. House of Representatives, Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, Mar. 22, 1989.
15. Elmer-Dewitt, P., ''The Perils of Treading on Heredity," *Time 70,* Mar. 20, 1989.
16. Ferrara, P. B., Virginia Bureau of Forensic Science, Richmond, VA, personal communication, May 1989.
17. Gelowitz, M.A., "DNA Fingerprinting: What's Bred in the Blood," *Criminal Reports* (3d) 65:122-135, 1989,
18. Goldman, J., American Civil Liberties Union, Washington, DC, personal communication, August 1989.
19. Gray, S.H., "Electronic Databases and Privacy: Issues for the 1990' s," *Science, Technology, and Human Values 14:3, 1989.*
20. Hicks, J.W., Federal Bureau of Investigation, testimony before U.S. House of Representatives, Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, Mar. 22, 1989.
21. Hicks, J. W., Federal Bureau of Investigation, "Conference Summary," International Symposium on the Forensic Aspects of DNA Analysis, Quantico, VA, June 23, 1989.
22. Hicks, J.W., Federal Bureau of Investigation, Washington, DC, personal communication, August 1989.
23. Horning, J.J., Goldman, J., and Gordon, D. R., "A Review of NCIC 2000: The Proposed Design for the National Crime Information Center," prepared for the U.S. House of Representatives, Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, February 1989.
24. Johnson, D. M., Federal Bureau of Investigation, "National Database Development," International Symposium on the Forensic Aspects of DNA Analysis, Quantico, VA, June 19-23, 1989.
25. Lander, E., Whitehead Institute for Biomedical Research, Cambridge, MA, personal communication, April 1989.
26. Laudon, K. C., *Dossier Society: Value Choices in the Design of National Information Systems (New* York NY: Columbia University Press, 1986).
27. McDonnell, M., Automated Microbiology Systems, Inc., San Diego, CA, personal communication, May 1989.
28. *Maney v. Ratcliff,* 399F. Supp.760(E.D. Wis. 1975).
29. Marchand, D. A., *The Politics of Privacy, Computers, and Criminal Justice Records* (Arlington, VA: Information Resources Press, 1980).
29. Marr, T. G., Los Alamos National Laboratory, Los Alamos, NM, personal communication, February 1989.
31. Marx, G.T, "I'll Be Watching You," *Dissent 32:26-34,* Winter 1985.
32. *Menard v. Saxbe, 498* F. 2d 1017 (DC. Cir. 1974).
33. Monson, K.L., "Semiautomated Analysis of DNA Autoradiograms,' *Crime Laboratory Digest 15:4, 1988.*
34. Monson, K. L., Federal Bureau of Investigation, Quantico, VA, personal communication, April 1989.
35. Moss, D. C., "DNA-The New Fingerprints," *ABA Journal 70,* May 1, 1988.
36. Mueller, L.D., University of California, Irvine, Irvine, CA, personal communication, August 1989.
37. National Crime Information Center, Minutes of the Advisory Policy Board Meeting, St. Petersburg, FL, Dec. 9-10, 1987.
39. New York State Forensic DNA Analysis Panel, "DNA Report," Sept. 6, 1989.
39. Nolan, K., and Swenson, S., "New Tools, New Dilemmas: Genetic Frontiers," *Hastings Center Report 18:5, 1988.*
40. *Paul v. Davis, 424* U.S. 693 (1976).
41. Peterson, J.L., testimony before U.S. Senate, Subcommittee on the Constitution, Committee on the Judiciary, Mar. 15, 1989.
42. Price, M. E., "Searching for a New Paradigm," *National Law Journal* Aug. 7, 1989, pp. 13-17.
43. Pun, T., Trus, B., Grossman, N., et al., "Computer Automated Lanes Detection and Profiles Evaulation of One-Dimensional Gel Electrophoretic Autoradiography," *Electrophoresis 6:268-274, 1985.*
44. Reeder, D.J., National Institute of Standards and Technology, Gaithersburg, MD, personal communication, June 1989.
45. Simon, P., "Chairman's Questions to the Panel," U.S. Senate, Subcommittee on the Constitution, Committee on the Judiciary, Mar. 15, 1989.

46. Smith, B. C., U.S. Army Central Identification Laboratory, Ft. Shafter, HI, personal communication, January 1989.
47. *Tarlton v. Saxbe, 507* F.2d 1116 (D.C. Cir. 1974).
48. Technical Working Group on DNA Analysis Methods (TWGDAM), *The Combined DNA Index System (CODIS): A Theoretical Model,* Federal Bureau of Investigation, Quantico, VA, Oct. 15, 1989.
49. Thompson, W. C., and Ford, S., "DNA Typing: Acceptance and Weight of the New Genetic Identification Tests," *Virginia Law Review 75:45-108, 1989.*
50. Trubow, G., *Watching the Watchers: The Coordination of Federal Privacy Policy,* Project on Communication and Information Policy Options, No. 5 (Washington, DC: Benton Foundation, 1989).
51. U.S. Congress, Office of Technology Assessment, An *Assessment of Alternatives for a National Computerized Criminal History System, OTA-CIT-161* (Washington, DC: U.S. Government Printing Office, October 1982).
52. U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-31O* (Washington, DC: U.S. Government Printing Office, October 1987).
53. U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy,* OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).
54. U.S. Congress, Office of Technology Assessment, "Issues Relevant to NCIC 2000 Proposals," staff paper, Nov. 12, 1987.
55. U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973.*
56. *United States Department of Justice v. Reporters Committee for Freedom of the Press, No. 87-1379,* decided Mar. 22, 1989.
57. Webb, J.E., Commander, U.S. Army Central Identification Laboratory, Ft. Shafter, HI, personal communication, January 1989.
58. Weedn, V., Office of Armed Forces Medical Examiner, Armed Forces Institute of Pathology, Baltimore, MD, personal communication, June 1989.
59. Westin, A. F., and Baker, M.A., *Databanks in a Free Society (New* York, NY: Quadrangle/The New York Times Book Co., 1972).
60. *Whalen v. Roe, 429* U.S. 595 (1977).