Chapter 1

Summary, Policy Issues, and Options for Congressional Action

"Positive identification by DNA profiling is fact. It is not subjective. It is not influenced by the vagaries of human emotion. "

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

"DNA fingerprinting is all but foolproof, but some fool is going to use it."

anonymous, August 1989

CONTENTS

Boxes

Figures

Tables

Chapter 1

Summary, Policy Issues, and Options for Congressional Action

Genetic uniqueness is a fact of life. From generation to generation, characteristics are inherited, combined, assorted, and reasserted among individuals through a common denominator: the chemical deoxyribonucleic acid, or DNA. And, except in the case of identical twins, no two humans share the same DNA sequence.

This report is about technologies used to distinguish the DNA among individuals. It is about techniques to identify and prosecute violent criminals, as well as exonerate innocent persons who are suspects in criminal cases. To a lesser extent, it is about applications that use the same techniques to determine parentage or identify and reunite missing children with relatives. Undertaken at the request of the Senate Committee on Labor and Human Resources, this assessment evaluates the scientific, legal, and ethical issues surrounding forensic applications of DNA tests: the validity and reliability of DNA tests for forensic casework, quality assurance and standards for DNA analysis by forensic laboratories, the legal basis for the admissibility of such tests in courts of law, privacy and civil liberties concerns about collecting, using, and storing genetic information and material, and criminal justice interest in employing DNA tests at the Federal, State, and local level.

TERMINOLOGY

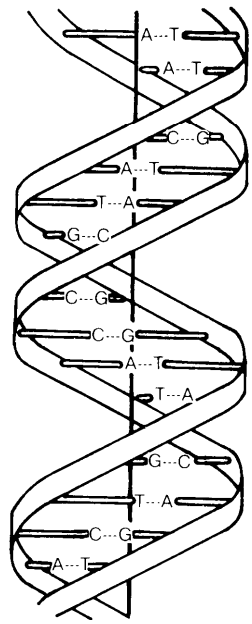
Forensic science involves the application of many scientific expertise (e.g., biology, chemistry, toxicology, medicine) to situations concerned with courts of justice or public debate. This report uses the term forensic applications to refer to potential uses of recombinant DNA technologies to identify individuals.

The increased acceptance and popularization of recombinant DNA techniques for forensic uses, especially criminal investigations, have led to some confusing terminology. In particular, some commentators have adopted the terms "genetic fingerprinting," "DNA fingerprinting, or "DNA prints" as generic phrases to describe all techniques, while others use the terms to describe specific techniques by specific companies. This report uses the terms DNA testing, DNA identification, DNA analysis, DNA typing, and DNA profiling to describe the two current and any future technologies, the practical goal of which is unique association or exclusion determined by DNA-based tests.

DNA AND HOW IT DIFFERS FROM PERSON TO PERSON

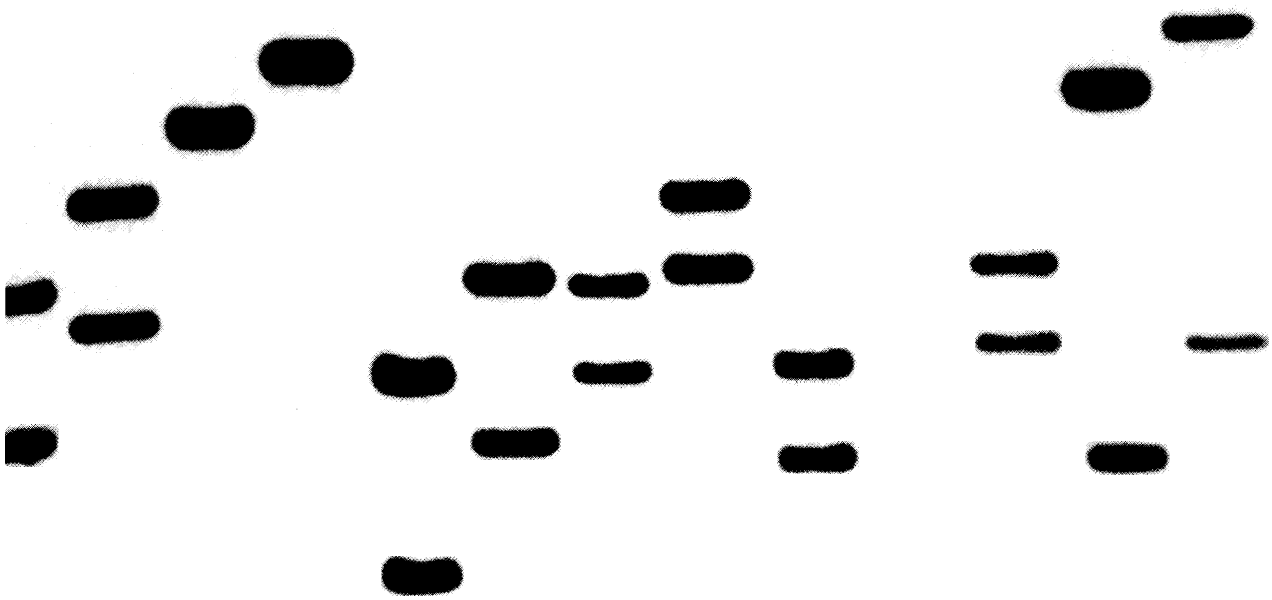
As the chemical dispatcher of genetic information, DNA's structure resembles a twisted ladder, referred to as a double helix (figure l-l). DNA in all organisms consists, in part, of four chemical subunits commonly called bases. These four bases—guanine (G), adenine (A), thymine (T), and cytosine (C)—are the genetic alphabet. Their unique order, or sequence, in the DNA helix serves as the blueprint for an organism. Of the 3.3 billion base pairs making up a human

Figure l-l—The DNA Double Helix



SOURCE: Office of Technology Assessment, 1990.

Figure 1-2—DNA Patterns From 12 Individuals



In this mock-up to demonstrate that DNA patterns differ among individuals, blood samples were obtained from 12 different people and RFLP analysis performed using 1 single-locus probe. Although some individuals do share 1 band in common, all 12 exhibit different patterns overall

SOURCE: Federal Bureau of Investigation, 1989.

blueprint, only a fraction—approximately *3* million—differ between any two individuals.

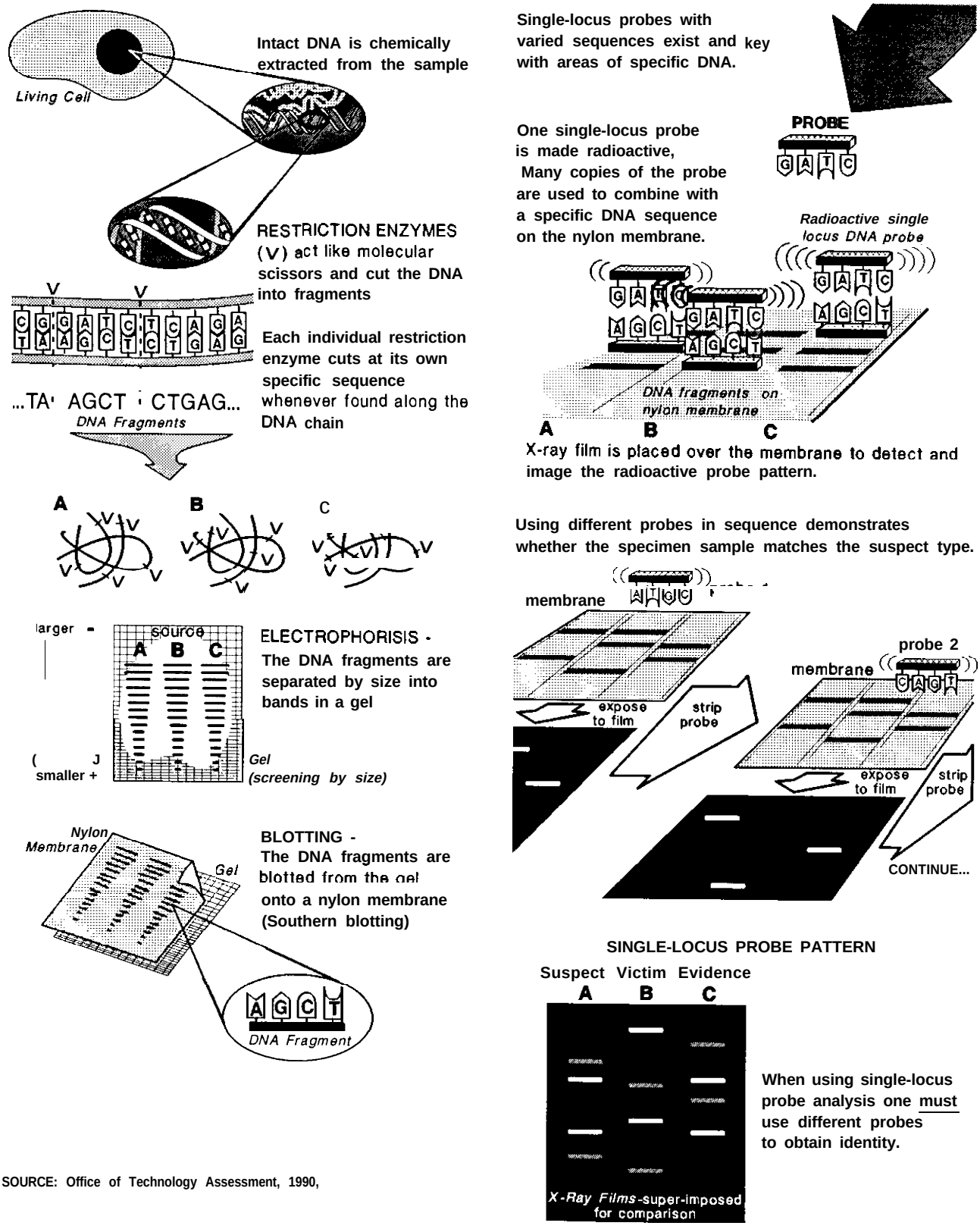
Several methods to detect DNA differences exist; the majority of DNA tests currently used in forensic applications detect some of these differences through DNA probes that reveal size variations. Scientists measure these size distinctions between people through a process called restriction fragment length polymorphism (RFLP) analysis (figures 1-2 and 1-3)[1]. Although the specific protocols used for RFLP analysis vary from laboratory to laboratory, the vast majority of forensic casework carried out today involves this basic approach.

Another technology, polymerase chain reaction (PCR), can be thought of in some respects as molecular photocopying (figure 1-4). PCR itself is not used to directly analyze DNA, rather it makes possible the application of other techniques when only minute biological specimens are available. PCR allows a scientist to take a sample of what ordinarily would be insufficient DNA to assess, and reproduce it until enough DNA copies are available for examination by a number of technologies, including RFLP analysis. Chapter 2 describes details of RFLP analysis and PCR.

DNA is found in all body cells except red blood cells. (Blood contains many cell types in addition to red blood cells, such as white blood cells, and it is from these cells that DNA can be obtained when forensic evidence is a bloodstain.) With few exceptions, the composition of a person's DNA does not vary from cell to cell, except in egg and sperm cells, which have half the complement of DNA present in other body cells. (Although DNA content differs from sperm to sperm, a DNA profile of semen-e. g., from evidence in a rape case—is a composite of thousands of DNA molecules from thousands of

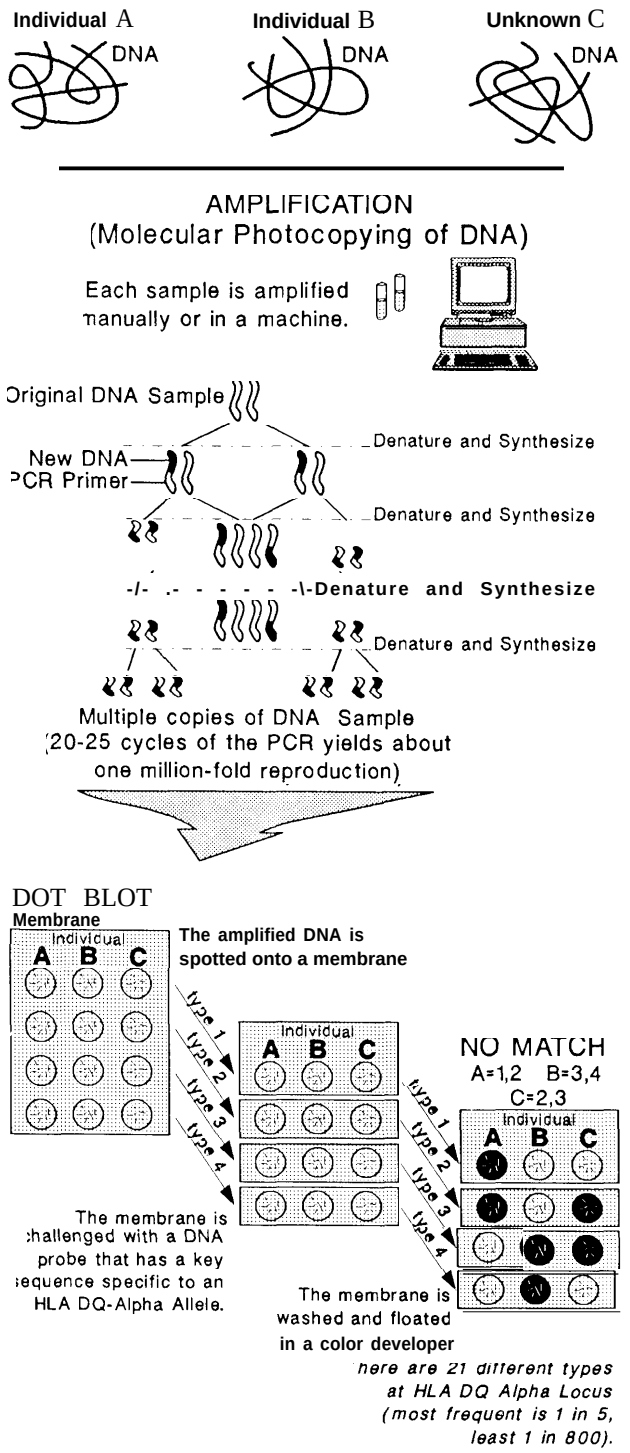
[1]The illustration of RFLP analysis involves the use of a type of DNA probe called a single-locus probe. A similarly performed analysis uses a different type of DNA probe, called a multilocus probe, which is only applied in some paternity cases in this country. Chapter 2 describes the differences between the two approaches. For purposes of this report—with the exception of chapter 2—RFLP analysis refers only to the use of single-locus probes.

Figure 1-3—Detailed Schematic of Single-locus Probe RFLP Analysis



SOURCE: Office of Technology Assessment, 1990,

Figure 1-4—The Polymerase Chain Reaction



SOURCE: Office of Technology Assessment, 1990.

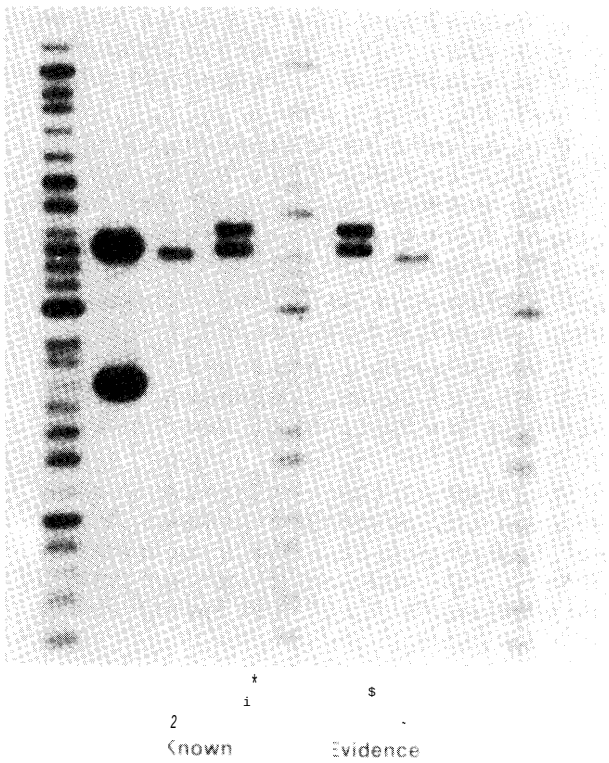
sperm and therefore reflects a man's overall profile (figure 1-5).) Thus a scientist can examine DNA from blood or tissue from a hair root and, if the specimens are from the same person, find the same DNA banding pattern. Similarly, patterns can be matched between DNA isolated from sperm on a vaginal swab or a semen stain and a known blood sample from a suspect.

THE ROLE OF DNA TYPING IN FORENSIC IDENTIFICATION

Traditional genetic markers, such as ABO blood groups, have been used in forensic casework since the turn of the century. Conventional markers available to forensic analysts provide the potential for a high degree of discrimination among different individuals, but the upper limit is attained infrequently, in part because of the instability of some of these markers in dried and aged evidence stains. Thus, in practice, the individualization of many evidentiary stains cannot be carried out to any great extent given the present array of conventional serological landmarks. In general, traditional genetic tests used in forensic casework also, at best, can associate an unknown sample with a suspect specimen at a level of 90 to 95 percent inclusion.

Forensic applications of DNA tests involve two components: molecular biology and population genetics. Molecular biological techniques allow analysts to directly examine the material responsible for heritable differences among humans, i.e., DNA. Population genetics, also a part of traditional forensic genetic testing, is used to interpret DNA tests to approximate the degree to which two samples are associated by greater than random chance. Like traditional genetic tests, DNA typing is used in the forensic context to determine whether biological material from a known individual can be linked to a sample from an unidentified specimen (i.e., whether the individual can be included in or excluded from the population of humans who could have deposited the biological material). Yet unlike traditional genetic testing, DNA typing technologies—one of which was first used in a criminal case in the United Kingdom

Figure 1-5—Example of One DNA Pattern in a Rape Case



Biological evidence from this rape case was separated by laboratory techniques into separate male and female fractions. After RFLP analysis of these fractions and known samples obtained from the victim and suspect, the results reveal that—for this particular probe-the DNA pattern of the male fraction matches the pattern of the suspect.

SOURCE: Federal Bureau of Investigation, 1989.

(box 1-A)—have been heralded as forensic tools that will change the judicial landscape.

It is the population dynamics of DNA markers that separates it from the use of conventional genetic markers in forensic analysis. With DNA markers, much greater variation exists and can be detected—hence their potential for what amounts to statistical individualization when a combination of markers is examined. That is, because the assortment of genetic markers detected by DNA tests is great, a sufficiently detailed examination of DNA patterns can yield a result that effectively amounts to a positive identification between a questioned sample and a suspect sample. By the same token, because DNA markers do vary so much, exclusion of innocent suspects can be easier to achieve. Forensic DNA analysis can provide more definitive and objective evidence to ascertain the innocence or guilt of an individual—especially compared to subjective evidence such as eyewitness testimony.

Forensic applications of DNA techniques are not limited to criminal investigations. Their use in parentage testing (figure 1-6), the identification of unknown remains, human rights abuses, and immigration has been successful. And as more information is gained through genetic research, including efforts to map and sequence the human genome, the range of applications, of information gained, and of technologies involved in forensic uses of DNA tests is likely to increase.

ARE DNA TESTS VALID AND RELIABLE?

An important matter in the use of DNA for forensic casework is whether the detection methods are scientifically valid. Validity is the probability that a test will correctly identify true matches and true nonmatches. For RFLP analysis, validity centers on whether the test yields the correct RFLP pattern. A valid test or set of tests in criminal applications, for example, would not falsely classify or exclude a subject by yielding a profile not true to type.

A second, but equally important aspect of DNA testing of forensic samples is reliability. Reliable tests measure reproducibly that which they are capable of measuring under defined conditions of use. Reliable methods must perform reproducibly within a laboratory, across multiple laboratories, and in the hands of disparate practitioners. Reliability involves several factors, including the procedures used, laboratory performance, laboratory recordkeeping, and quality control and quality assurance.

Genetic and molecular principles underlying DNA identification are solid and can be applied to DNA isolated from forensic evidence. The Office of Technology Assessment (OTA) finds that forensic uses of DNA tests are both reliable and valid when properly performed

Box I-A—The L.eicester 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 1+," 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 kmown 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 Nov. 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 mate 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.

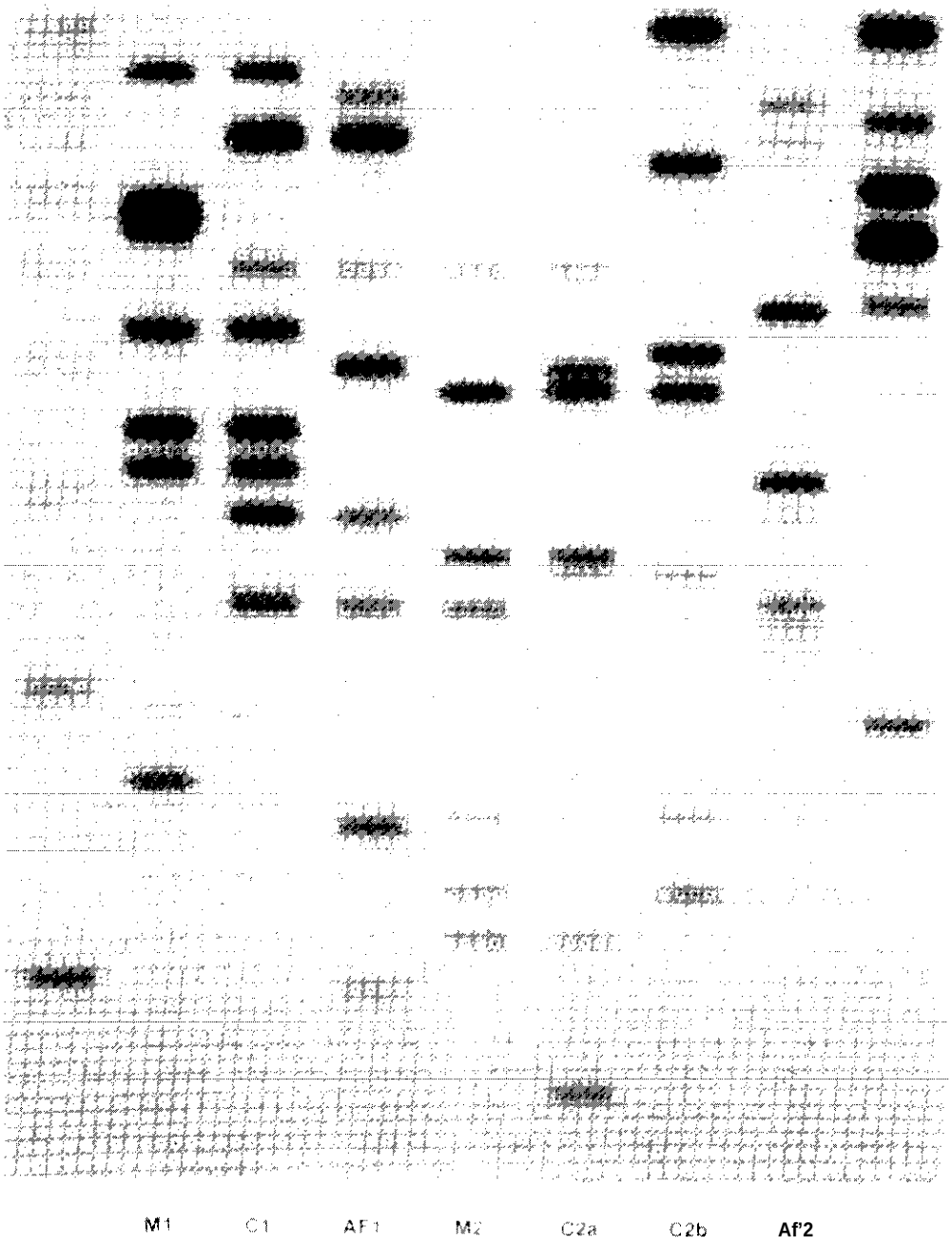
Pitchfork received a double life sentence for the murders, a 10-year sentence for each of the rapes, 3 years each for two earlier sexual assaults, and 3 years for conspiracy, all to be served concurrently. The concurrent sentences mean he could be released within 10-12 years. At sentencing, the judge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

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

and analyzed by skilled personnel. Molecular genetics techniques can accurately disclose DNA patterns that reflect DNA differences among humans. Questions about the validity of DNA typing-either the knowledge base supporting technologies that detect genetic differences or the underlying principles of applying the techniques per se—are red herrings that do the courts and the public a disservice. Critical questions about the reliability of DNA testing, however, have been raised in a few cases. Challenges to the reliability of DNA tests will mount unless the issue of standards is addressed.

The validity of forensic DNA tests does not hinge on population genetics. Interpretation of test results, however, depends on population frequencies of the various DNA markers (for

Figure 1-6—DNA Typing in Two Paternity Cases



DNA typing in two different paternity disputes revealed that the alleged father (AF) is the biological father in case 1, but not in case 2. Note that all bands present in the child in case 1 (C1) can be accounted for in either the mother (M1) or alleged father (AF1). In case 2, however, no bands from the alleged father (AF2) appear in either child (C2a and C2b), nor do bands that the children do not share with their mother (M2) match any present in the alleged father (A2).

SOURCE: Cellmark Diagnostics, 1989.

RFLP analysis, the size of the band in a particular test). In other words, population genetics provides meaning—numerical weight—to DNA patterns obtained by molecular genetics techniques. Given any set of patterns, or just two patterns, that match, population frequencies are used to report the frequency of such an event arising; they are key to establishing confidence in associating an unknown evidence pattern with that of a suspect—for example, whether 1 in 30 billion, 1 in 2 million, 1 in 50, or 1 in 10 random individuals could be expected to share that test result. That scientific principles of population genetics can be applied to forensic DNA analysis is not in question, but how best to apply which principles to RFLP analysis is under debate. Disagreement exists as to the extent such debate can or should be resolved. General agreement does exist that any potential bias that could result from calculating population frequencies favor a defendant. Some argue, however, that the magnitude of the number is not the issue, just that the analyst assigns it with scientifically valid confidence. Others argue that because of the pivotal role population frequencies can play in reporting results of forensic DNA tests, agreement is necessary.

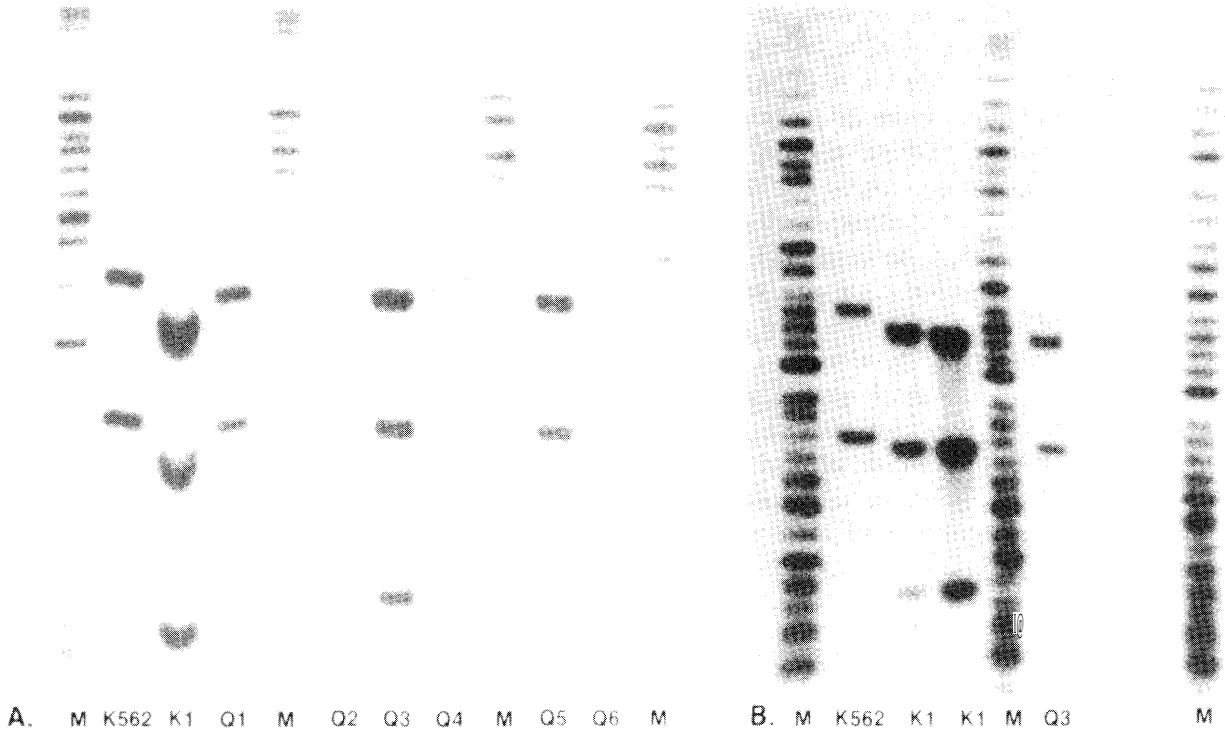
STANDARDS

Although consensus exists that the power of DNA typing technologies to theoretically individualize is valid and reliable, a constellation of recommendations are offered on how best to implement forensic uses of DNA tests. These opinions focus on the most effective way of minimizing realistic technical variability, human error, and the vagaries of working with specimens obtained under less than ideal conditions (figure 1-7). Such differences underscore the urgent need to develop both technical and operational standards. Setting standards for forensic applications of DNA testing is the most controversial and unsettled issue. Standards are necessary if high-quality DNA forensic analysis is to be ensured, and the situation demands immediate attention. Leaving the issue of standards unresolved places a burden on all parties involved in forensic DNA analysis. Undoubtedly some queries will still arise on a case-by-case basis, and at such times specific details can and should be evaluated in court. Given time and the implementation of standards, such questions are likely to decrease.

The Federal Bureau of Investigation (FBI), industry, research molecular biologists, population geneticists, and forensic scientists agree that standards are desirable. For many matters, however, little agreement exists on who should decide, what standards are best, and how to achieve and implement them. OTA identified two types of standards: technical and operational. The former include such issues as proper reagents and gel controls; electrophoresis conditions; rules to match DNA banding patterns; the extent that computer-assisted matching should be permitted; and population data to compute the likelihood of matches. Operational standards include elements such as recordkeeping and proficiency testing; they are likely to be more controversial than technical standards, for historically, attempts to regulate laboratory practices in any sector have met with resistance. (Quality assurance most directly addresses many issues in operational standards and is discussed in the following section.)

Technical standards that allow flexibility for laboratory-to-laboratory variations need to be evaluated. Clearly defined rules and procedures—objective and scientifically based—should be established, set, and, most importantly, followed. One critical area lacking full agreement is that of declaring matching patterns in RFLP analysis. For example, calling a match or nonmatch can be difficult if a pattern in the evidence is similar, but off-set, or shifted, compared to a suspect sample. Agreement is desirable on what the best, and the minimal, mechanisms are to control for potential anomalies so that data interpretation is still possible if situations such as band-shift arise in a particular case. With PCR, minimum standards and controls to avoid contamination that could lead to erroneous interpretation should be determined.

Figure 1-7—DNA Typing and Murder: A Less Than Ideal First Analysis and a Solution



n this murder case, six separate pieces of evidence were obtained from the crime scene and a suspect identified. RFLP analysis was ɔerformed (M=markers; K1=suspect; Q1-6=evidence; K562=standard), but the results revealed that too much of the suspect sample (K1) ıad been placed on the gel, which led to distortion in the K1 lane, as well as the lanes next to it (K562 and Q1) (panel A).

Even though the suspect's pattern for this probe is an extremely rare and unusual three-band pattern that is similar to the six questioned samples, the forensic analyst cannot call a "match," but must report the test "inconclusive" because the alignment is unacceptable. This, despite knowing from experience that if less suspect sample had been used, the patterns likely would have aligned and been called a match.

Fortunately, not all of evidence sample Q3 had been used in the test in panel A (although Q1,2,4-6 had been exhausted). The case was repeated (panel B) with diluted amounts of the suspect sample (K1), which now clearly align with the evidence pattern (Q3). Had no evidence sample been available for an additional try, however, DNA analysis would have reported "inconclusive," and could not have been used as evidence to prove guilt or innocence.

SOURCE: Federal Bureau of Investigation, 1989.

Decisions about standards in forensic applications of DNA tests need to be made within the constraints of performing DNA analysis on case samples, but achieved without compromising scientific and technical integrity. For example, some feel that mixing tests (used to determine if two apparently identical RFLP samples that are run side-by-side actually run as one when mixed) are critical. Others strongly feel alternative controls provide enough safeguards and that mixing tests are impractical for most forensic casework—particularly when material may be limited.

QUALITY ASSURANCE

Quality assurance mechanisms in forensic uses of DNA profiling encompass a range of options, including certification, licensing of facilities and personnel, accreditation, recordkeeping, and proficiency testing. Professional societies, State and local Governments, and the Federal Government all have or could have roles in ensuring high-quality forensic DNA typing services. Similarly, numerous methods are available to these entities to implement an assortment of options.

Professional societies can set informal standards and encourage voluntary compliance, and several organizations have developed or are developing guidelines for quality assurance for forensic applications of DNA tests. Many professional societies have a stake in quality assurance of DNA typing for forensic applications, and cooperation between them could be a powerful mechanism to ensure high-quality analysis. On the other hand, because such efforts are voluntary, some criticize current optional programs as insufficient, and note that professional society membership or claims of adherence to different professional guidelines can sometimes confuse lay observers and should not be viewed as the ultimate imprimatur of quality assurance. For forensic science, only one voluntary accreditation program is offered—by the American Society of Crime Laboratory Directors.

In addition to the role professional societies can play, States have the authority to regulate DNA typing by both public and private laboratories. Presently, no State has enacted general licensing requirements for private laboratories, crime laboratories, or personnel performing DNA analysis on forensic specimens, although a September 1989 report by a special commission appointed in New York made recommendations in each of these areas. (In contrast, all 50 States and the District of Columbia require that public and private hospitals be licensed, although the scope of the laws varies considerably.)

The Federal Government has broad authority to direct that solutions be found for quality assurance issues surrounding forensic uses of DNA tests. Federal leadership can focus on nonregulatory mechanisms, or Congress and the executive branch could move to directly regulate crime laboratories, as it has for drug testing facilities (box l-B) and clinical laboratories (box l-C). Some feel, however, that legislation like the Clinical Laboratory Improvement Amendments of 1988 (CLIA) (Public Law 100-578) is more a short-term solution—that, in fact, court conflict, as is presently occurring, sharpens the examination and evaluation of forensic DNA typing and will ultimately ensure quality by defining its boundaries. Moreover, questions are raised whether high-quality necessarily follows from mandatory regulation.

Nonregulatory Federal efforts could focus on authorizing additional efforts for research in forensic sciences, particularly cross-disciplinary projects that apply newly emerging basic research tools to real-world casework. Other nonregulatory Federal initiatives can encourage the use of consensus conferences to develop and recommend protocols for quality assurance. This role in particular, perhaps modeled after the existing National Institutes of Health (NIH)

Box l-B-Quality Assurance and Drug Testing Laboratories

***Drug* testing** of employees and job applicants has become increasingly commonplace. The dramatic increase in testing facilities to handle samples has spawned concern about ensuring that sufficient **care** is taken so that those tested are not harmed by poor-quality tests or inadequate quality assurance policies or quality control procedures. In 1988, the General Accounting Office surveyed all 50 States on the nature of laws, regulations, and other legally enforceable provisions in effect that would govern quality assurance of drug testing laboratories. The survey revealed that no uniform system exists to regulate laboratories doing employee drug testing. Some States do have formal mechanisms specific for quality assurance oversight of drug testing facilities. Others regulate laboratories that perform employee drug analysis through general medical or clinical laboratory statutes. Still others voluntarily adhere to standards prescribed by various professional associations. Some do not control such services at all.

The executive branch has moved to improve results from laboratories providing employee drug testing services (53 FR 11970, Public Law 100-71). Congress also is interested in ensuring quality in laboratories that do employee drug testing, Legislation considered during the 100th Congress would have required proficiency testing and certification by the U.S. Department of Health and Human Services for all facilities engaged in urinalysis and blood analysis for employee drug testing. Similar legislation is pending in the 101st Congress.

SOURCE: OffIce of Technology Assessment 1990.

Box l-C-Quality Assurance and Clinical Laboratories

In October 1988, Congress passed sweeping legislation that subjects clinical laboratories to a number of requirements, including qualifications for the laboratory director, standards for the supervision of lab testing, qualifications for technical personnel, management requirements, and an acceptable quality control program. Prior to enacting the Clinical Laboratory Improvement Amendments of 1988 (CLIA) (Public Law 100-578), Federal regulations covered the approximately 13,000 labs that either transported samples between States or performed tests billed to Medicaid and Medicare. Beginning in 1990, however, the Health Care Financing Administration (HCFA) of the U.S. Department of Health and Human Services (DHHS) wilt exercise sweeping regulatory authority over clinical laboratories. HCFA will set standards for staffing and maintaining all medical laboratories, including physician office testing. HCFA will also manage a comprehensive program to police the facilities and can impose sanctions.

CLIA is at once broad, encompassing the estimated 98,000 physician labs, and specific. For example, the Secretary of DHHS is to establish national standards for quality assurance in cytology services, including the maximum number of cytology slides that any individual may screen in a 24-hour period. The Secretary is also required to determine and implement recordkeeping, inspection, and proficiency testing programs, and to study and report to Congress on a range of issues gauging the impact of various quality assurance mechanisms.

CLIA expands DHHS's regulatory authority over clinical laboratories, and grants HCFA the power to suspend or revoke a lab's certificate for violation of the rules. Further, fines up to $10,000 for each violation or each day of noncompliance can be levied, and jail sentences of 3 years can be imposed. The law continues to permit, subject to approval by the Secretary, the involvement of State or private nonprofit associations (which at present include the College of American Pathologists, the American Association of Bioanalysts, agencies in 3 States, the Joint Committee on Accreditation of Healthcare Organizations, and the American Osteopathic Association) to substitute for the Federal regulatory process.

Prior to CLIA's enactment, one issue of critical concern to Congress was proficiency testing programs. Until CLIA, such programs varied broadly in testing criteria and in grading of test results. Moreover, uniform or minimally acceptable Federal standards did not exist. Now, except under certain circumstances, proficiency testing shall be conducted on a quarterly basis, with uniform criteria for all examinations and procedures. The Secretary shall also establish a system for grading proficiency testing performance.

SOURCE: Office of Technology Assessment **1990.**

consensus conference process, could be effective in addressing outstanding controversies surrounding forensic applications of DNA testing. Another structure, the NIH Recombinant DNA Advisory Committee, could be used as a model structure for Federal oversight or regulation of forensic DNA analysis.

One specific nonregulatory effort in place involves the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, a neutral Federal agency and the only Federal laboratory with the explicit goal of performing research in and providing reference standards. As a significant part of quality assurance involves confidence in measurement standards, proposals put forth by NIST to examine state-of-the-art gel electrophoresis, reagent quality, electrophoresis conditions, and evaluation of size markers could be important.

Another nonregulatory Federal initiative presently under way is the FBI's Technical Working Group on DNA Analysis Methods (TWGDAM), which among other issues is examining quality assurance, population statistics, and databanking. Consisting of representatives of crime laboratories at or near implementation of DNA profiling techniques, as well as of commercial laboratories, TWGDAM has been praised by some as the nucleus around which national expertise will develop. Other have criticized it for being generally closed—by invitation only—in its early stages of decisionmaking. Some, both within and outside the forensic science community, are bothered that any largely investigative and enforcement body serve as the lead player in developing standards in which it has a vested interest. For many, TWGDAM represents the first step in a probable

multistage process that will unfold as efforts to ensure quality of forensic applications of DNA typing develop.

Instituting quality assurance mechanisms should proceed without delay. Accreditation, licensing, and certification are among the mechanisms of quality assurance that could be applied to facilities performing forensic DNA analysis. Such initiatives individually, or as a package, do not guarantee high-quality DNA typing, but some effort appears necessary to assist private laboratories, the Federal Government, courts, and crime laboratories. Further, any program must be flexible for two reasons: to address the inherent variability of forensic casework and to account for the evolution of existing technologies and emergence of new ones. These endeavors also must acknowledge that introducing and maintaining formal quality assurance mechanisms can be costly and time-consuming, and will place additional staffing and financial burdens on public facilities already overwhelmed with casework and historically underfunded. And, while some argue that standardizing DNA typing is an additional layer of quality assurance, standardization clearly is most important to computer databanking issues (discussed in a following section).

Finally, nothing is routine during the course of a forensic investigation. Thus, no amount of standardization, standard setting, or quality assurance can be substituted for appropriate interpretation and analysis by a forensic scientist during the course of an individual case. Federal leadership in providing adequate and proper education and training, perhaps confirmed through certification or licensing, would enhance forensic DNA analysis across the country, although improved training and education should not be viewed as substitutes for the implementation of standards.

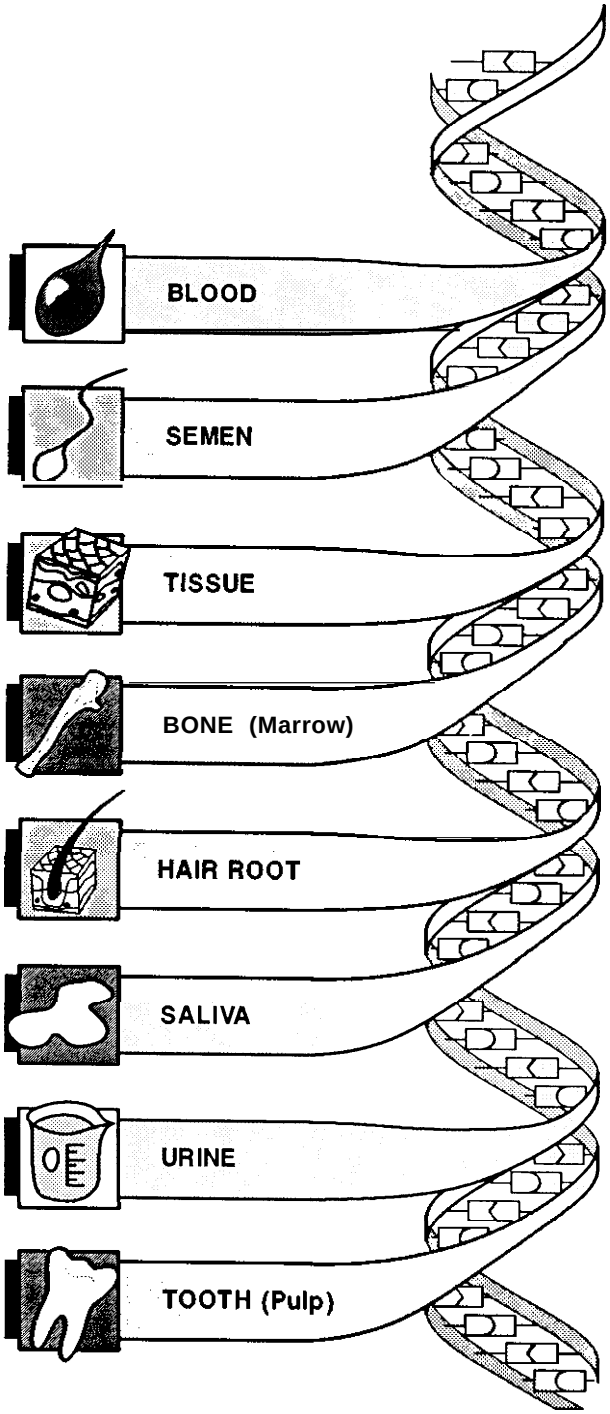
DNA IN COURT

In courtrooms, DNA testing is a recent and highly touted evidentiary tool (figure 1-8). First introduced into U.S. criminal proceedings in ***1986,*** forensic DNA analysis has since been admitted into evidence in at least 185 cases by 38 States and the U.S. military as of January 1, 1990 (table 1-1; figure 1-9). This number does not reflect its even wider use in investigations that did not go to trial; although impossible to precisely determine, OTA estimates that, to date, DNA tests have been used by law enforcement in over 2,000 investigations. OTA found DNA tests were used for criminal investigations and proceedings in at least 45 States and the District of Columbia as of January 1, 1990. Nor do the numbers reflect the use of DNA tests in thousands of paternity disputes annually. Three private laboratories and the FBI provided expert testimony in 216 criminal cases as of January 1990. Court-appointed and privately retained experts, and State law enforcement personnel also have testified.

Although the admission of DNA testing in courts is a new phenomenon, scientific evidence is not. Both, however, present a special dilemma because they usually involve technical information ‘‘beyond the ken” of the average citizen. To address this situation, Congress, States, and many courts have created standards governing the admission of such information into evidence in courts. Generally involving expert scientific testimony, two rules address the admissibility of scientific evidence, including DNA typing, into U.S. courtrooms: The Frye test and the relevancy test. Both are designed to deduce, through analysis and the testimony of expert witnesses, whether the scientific test in question is reliable. In addition, some States have passed specific laws addressing the admissibility of certain scientific techniques, for example, radar or intoxication tests. As of January 1990, four States, Maryland, Minnesota, Louisiana, and Nevada, have passed laws addressing the admissibility of DNA typing.

Under the Frye standard, which is the oldest and most often used test in determining the admissibility of scientific evidence, courts admit evidence based on a scientific technique only when the technique has gained general acceptance in the relevant scientific community.

Figure 1-8—Sources of DNA Evidence



SOURCE: Office of Technology Assessment, 1990

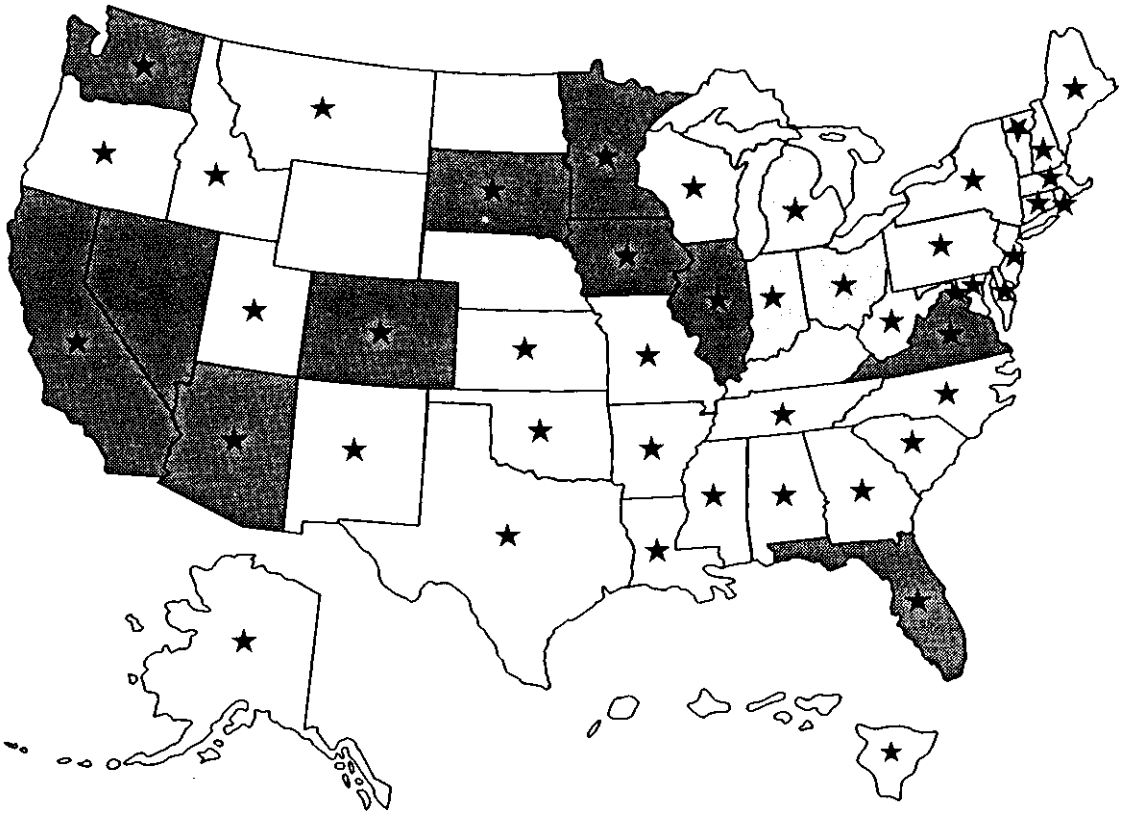
Table I-l—Number of DNA Cases by State[a]

State	Number of cases
Alabama	6
Alaska	—[b]
Arizona	3
Arkansas	1
California	8
Colorado	7
Connecticut	1
Delaware	1
District of Columbia	—[b]
Florida	25
Georgia	4
Hawaii	1
Idaho	1
Illinois	1
Indiana	3
Iowa	2
Kansas	5
Kentucky	—[c]
Louisiana	1
Maine	—[b]
Maryland	11
Massachusetts	1
Michigan	5
Minnesota	2
Mississippi	4
Missouri	2
Montana	1
Nebraska	—[c]
Nevada	—[c]
New Hampshire	2
New Jersey	—[b]
New Mexico	—[b]
New York	17
North Carolina	4
North Dakota	—[c]
Ohio	10
Oklahoma	3
Oregon	1
Pennsylvania	9
Rhode Island	—[b]
South Carolina	4
South Dakota	1
Tennessee	1
Texas	18
Utah	1
Vermont	—[b]
Virginia	10
Washington	4
West Virginia	1
Wisconsin	1
Wyoming	—[c]

[a]Where such evidence was admitted by a court or used to obtain a plea prior to an admissibility hearing. Total of 185 cases includes two military cases not reported in this table (see app. A).
[b]Case pending, DNA used for exculpation only, DNA evidence withdrawn, or DNA used in investigation, but no prosecution.
[c]None identified.

SOURCE: Office of Technology Assessment, 1990.

Figure 1-9—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.

Although criticized because ''general acceptance' may not equate with scientific reliability, proponents note that the Frye test guarantees a minimal amount of support by experts for a scientific test or procedure prior to allowing cutting-edge technology into legal deliberations. Under the relevancy test, which is based on the Federal Rules of Evidence originally promulgated by the Supreme Court and affirmed by the Congress in 1975 (Public Law 93-595), scientific evidence is admissible if it is relevant and helpful to the judge or jury hearing the case. Among other conditions, the trier-of-fact must have the technical expertise to assess properly the reliability of the scientific testimony of the expert witness (and the evidence thus be helpful). Applied in all Federal courts, the relevancy test also serves as the standard for admissibility of scientific evidence in non-Federal courts in 32 States.

The admissibility of DNA testing as evidence under the Frye test v. the relevancy test is of limited significance. The 185 cases identified by OTA indicate that in using either criteria courts find DNA typing technologies per se to be generally accepted by the scientific community, or relevant and helpful to judges and juries. No State court has found that DNA testing per se fails to meet established tests for admissibility, although in some cases the admissibility of DNA evidence has been limited or barred. Although DNA currently intro-

duced as evidence is evaluated case-by-case, some argue that as more acceptance occurs a carte blanche for the admissibility of DNA typing evidence could soon be seen. Nevertheless, because aspects of forensic DNA analysis are receiving increased scrutiny, future court considerations will hinge on standards and quality assurance in forensic applications of DNA tests.

Even before determining whether biological evidence meets established grounds for admissibility, some argue that constitutional considerations in obtaining such evidence need to be considered; in particular, that Fourth, Fifth, Sixth, and Fourteenth Amendment issues of search and seizure, self-incrimination, right to counsel, and due process (respectively) should be raised. Although a comprehensive examination of constitutional issues is beyond the scope of this report, it appears that DNA testing as evidence for identification is unlikely to be viewed as presenting special constitutional considerations-in particular, as violating Fifth, Sixth, and Fourteenth Amendment rights. In the case of rights against unreasonable search and seizure, OTA identified one appellate-level case involving DNA typing where the issue was raised, but the court did not review the claim that the taking of a blood sample violated the Fourth Amendment since the defendant had consented to the procedure. In any case, search and seizure of evidence for DNA typing is unlikely to center on issues unique to DNA evidence.

ADVANTAGES AND LIMITATIONS OF DNA TYPING AS EVIDENCE

DNA testing for identification purposes affords several advantages to the law enforcement and the legal system and no disadvantages per se. In the United States, high violent crime rates often yield biological evidence, but traditional serological technologies achieve only modest success in either associating or disassociating suspects with the crime. DNA identification is likely to influence and build on present-day success with such traditional forensic genetic technologies.

As a biological material distinguishing individuals, DNA is more variable and stable, and detection methods more robust, than traditional genetic markers examined by forensic laboratories. As an index of differentiation between two humans, it is also more powerful than conventional markers because it can provide what amounts to a statistically positive link between an individual and biological evidence from a crime scene. And, because it is more discriminating, it is also easier to clear wrongly accused persons. For example, approximately 37 percent of the cases received by the FBI for DNA analysis result in exclusion of the primary suspect.

DNA testing can save law enforcement and courts time and money by exonerating innocent suspects before trial, or through plea bargaining for guilty parties, as increasingly defendants are confronted with DNA typing results. DNA profiles can also be stored in a computer network that could subsequently be used to investigate rapes and serial crimes. In 1988, 92,486 forcible rapes were reported, and studies indicate that this number is an underestimate since fewer than half of rape victims report this crime. In terms of impact on convictions or acquittals, sexual assault cases are most likely to reap the benefits of DNA typing.

No disadvantages of DNA testing technologies themselves were identified by OTA, but limitations and criticisms exist. In 1988,20,675 murders and nonnegligent manslaughter cases were reported in this country, and although forensic analysis using DNA typing in specific homicide cases certainly will be useful, its effect on aggregate homicide solution rates might not be appreciable, except perhaps in serial murders. Critics argue that DNA testing has been rushed into court without agreement being reached in the scientific community regarding either standards that ensure the reliability of the evidence or guidelines for interpreting results. And, because DNA testing itself and the costs associated

with expert witnesses can be substantial, the ratio of defense to prosecutorial resources, already heavily in favor of the prosecution, could be widened. Finally, many harbor the misconception that DNA typing applied to forensic samples always yields a "yes" or ''no answer. Tests are not black and white, and DNA profiling tests are no exception. An important, and often overlooked, result of an analysis could be ''inconclusive, ' ''uninterpretable, or ''uninformative, ' which should not be misconstrued as either inclusion or exclusion of a suspect. Nor does any matching profile necessarily mean positive identification, since the power of DNA analysis depends on the population characteristics of the tests used.

COMPUTER TECHNOLOGY AND DNA IDENTIFICATION

Computer technologies are central to forensic applications of DNA typing in two respects. First, computers can be used to more objectively and precisely analyze results of DNA typing, including RFLP analysis. Second, computers can be used to store DNA typing results. Databanking of DNA profiles can be used to either collect population statistics, which leads to more accurate estimates of the frequency that a particular DNA pattern occurs in a population, or to provide criminal investigative support.

In the area of analyzing DNA test results, computers help scientists by both speeding the process and employing computational tools to augment the power of the human eye. Because the actual readability of x-ray films, which are the final units depicting an individual's stripe-like pattern, varies from case to case, computers are used to reduce human discrepancies. Without computers, analysts ''eyeball' banding patterns on x-ray films—potentially leading to more subjective results from analyst to analyst, or even for the same individual.

A range of computer systems exists for RFLP analysis, and the amount of analyst-computer interaction is tremendously diverse. One system involves the individual marking the location of bands, then allowing the computer to calculate whether known and questioned samples match. In another, more-automated system, the computer automatically marks band positions it detects through a video camera and image analysis. Such systems can also apply mathematical algorithms to normalize band patterns, ''straighten' lanes, account for inconsistent gel composition, variation in electric field, or other conditions prior to calculation of fragment size. Computers can, without operator involvement, discriminate banding patterns not detectable with the human eye alone. Yet while they can assist in identifying legitimate bands, computers can also be influenced by background noise and create, even in controlled situations, a result where none was expected. Computer-assisted analysis of RFLP patterns is under way at commercial firms and at FBI, State, and local laboratories.

Computer-assisted image analysis of DNA tests, while useful, raises the question, do computers lie? Depending on the level of computer v. analyst interaction in analyzing DNA testing data, special consideration may be necessary in judicial deliberations. Forensic analysts, not computers, will appear in court for examination as witnesses. The forensic science community may want to ensure that analyst-computer integration can be traced so that edited patterns can be reconstructed, and that the initial image is available for review by another individual. Courts could be required to determine the admissibility of computer-enhanced images—cleaner and, arguably, more persuasive than typical x-ray film—and will need assurances that such images are an accurate representation of a test's results. Thus, both courts and the forensic science community should be prepared for future discussions on whether to subject computer analysis tools to verification and reliability testing analogous to those applied to DNA technologies.

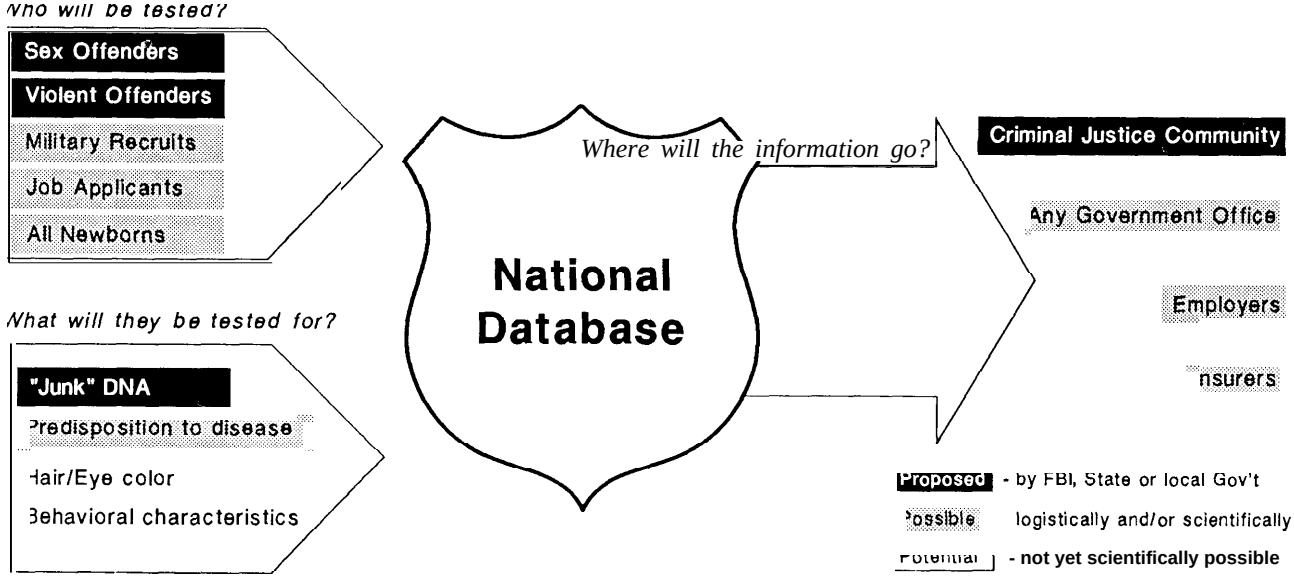
In the second area of utility, databanking, computer technologies enhance the ability of Federal, State, and local law enforcement officials at many levels (figure 1-10). The auto-

mated fingerprint identification system, for example, has revolutionized the ability of criminal investigators to identify suspects within and across jurisdictional boundaries. Similarly, considerable interest exists in using computer technologies to enhance criminal investigations through datasharing of DNA test results. Centralized or linked databases containing DNA profiles would permit rapid, electronic comparison of results from tests on different samples within a laboratory and among laboratories nationwide. An OTA survey of State and local crime laboratories revealed a large majority of laboratories (95 percent) said that DNA results should be incorporated into a database for exchange among law enforcement agencies.

As mentioned earlier, databanks are being used to store information to generate population genetics data to support RFLP analysis. Databases for population statistics purposes arouse little controversy; computer storage of investigative support data are more controversial. (See following section on privacy.) The FBI is currently developing a theoretical model and working prototype for an investigative DNA profiling database. At least three types of information files would be included: open case, missing persons/unidentified deceased, and convicted offenders. The former two types would be centrally maintained by the FBI. Open case files could be used to help investigators determine if a series of crimes were committed by the same person. Missing persons/unidentified deceased files could include DNA information from parents who report their children missing, so that as children are located, the child's DNA can be compared with parental DNA profiles on file. Convicted offenders files would be maintained by individual States, but the FBI would provide an indexing service, with States capable of gaining access to other States' files after certain approvals were obtained (figure 1-1 1). Sixteen States and one county have authorized or initiated legislation to authorize known offenders files (table 1-2).

Because a cross-jurisdictional network will be required to maintain proposed investigative databases, discussions are being held about the

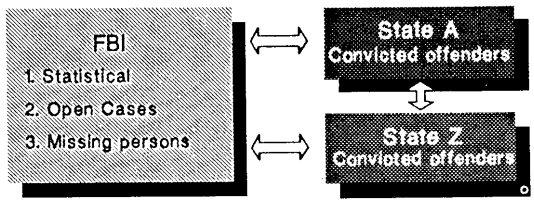
Figure 1-10—How a Database of DNA Information Could Be Created and Used



The law enforcement community cites a need for a DNA database to apprehend repeat offenders and solve serial crime; 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.

Figure I-ll—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.

most appropriate mechanism. DNA data held in Federal, State, or local files could be exchanged through the National Law Enforcement Telecommunications System (NLETS). A computerized message switching network operated by a nonprofit corporation controlled by the States, NLETS does not hold or manage data files, but is a possible vehicle for DNA data transmission. The most likely candidate to handle interjurisdictional inquiries is a system maintained by the FBI, the National Crime information Center (NCIC). NCIC currently contains about 20 million records on persons and property, and answers almost instantly about 75,000 inquiries a day. Although in December 1987 the NCIC Advisory Policy Board voted not to add DNA information to NCIC at that time, DNA testing and acceptance by law enforcement has spread rapidly since then. In June 1989, the Board reconsidered its actions, voting to index and match DNA profiles in NCIC.

Another area related to databank development (as well as to standards of statistical analyses) where many agree attention should be focused results from the dynamic and diverse nature of the U.S. population. Collection, classification, and databanking of genetic differences based on ethnic and racial subgroups affects efforts geared toward both population statistics and investigatory databanks. Stratification based on self-reporting or surname (e.g., Hispanic) can be misleading. If future investigatory databanks rely on such information to associate a certain DNA banding pattern from an unknown sample

Table 1-2-State Laws To Establish Computer Files of Known Offender Genetic Patterns[a]

State	Action
Arizona	Governor signed a 1989 law requiring DNA testing of convicted sex offenders.
California	Passed laws in 1985 and 1989 requiring all convicted sex offenders to provide blood and salivia specimens at the time of their release from prison. Samples collected to date and future samples will be submitted for DNA testing, and the Attorney General's Office has begun studies to determine the best methods for collecting and storing data.
Colorado	Enacted legislation to require genetic testing of all sexual assault offenders released on parole after May 29, 1988.
Florida	A law enacted in 1989 calls for a computer bank for genetic information on convicted rapists.
Illinois	Legislation enacted requiring those 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	Governor signed a law in 1989 that permits DNA testing in the criminal law context. The Attorney GeneraJ's Office will issue rules about which crimes are covered and who will be required to donate DNA samples. Genetic profiling could become a rendition of parole.
Minnesota	Law enacted in 1989 that requires uniform procedures for collecting DNA information in cases of criminal sexual conduct, requires a court that is sentencing a person for criminal sexual conduct to order a DNA analysis specimen, and provides for admission of DNA test evidence without expert testimony.
Nevada	Requires that convicted sex offenders submit to DNA testing of their blood and saliva, and requires that the test results be maintained in the State's criminal history records.
South Dakota	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 and arrested.
Virginia	State legislature passed a bill in the 1989 session that requires DNA typing of convicted sex offenders.
Washington	State law requires a system to collect genetic descriptions of violent and sexual offenders. In addition, King County (Seattle) passed an ordinance requiring DNA testing of sex offenders.

aAs of January 1990, at least five other States-Connecticut, Massachusetts, Michigan, Indiana, and Ohio-have proposed DNA databanking legislation that had not yet been enacted.

SOURCE: Office of Technology Assessment, 1990.

to a racial or ethnic group, problems will likely arise.

Finally, DNA test results have been successfully computerized, but unless methods are standardized, e.g., restriction enzyme and probes, the potential usefulness of known offenders files or missing persons files will be constrained. Although no insurmountable technical difficulties face databank development, without quality control and quality assurance for DNA typing itself, without computer compatibility, institutional protocols to review results before data entry, and a capability to handle new DNA typing developments, computer technology combined with DNA analysis as a tool will be limited. Some postulate that the push to establish investigatory databanks will, by itself, be the factor that leads to standardization and quality assurance.

PRIVACY AND CIVIL LIBERTIES CONSIDERATIONS

As long as information refers to an identifiable individual—whether that reference is made by a person's name, a number, or some other distinguishing characteristic-it is personal information. The pervasive use of computer systems to collect personal information raises civil liberties issues and informational privacy concerns. Social security numbers are personal, as are fingerprints. Use or misuse of personal information collected in electronic databases can affect an individual's ability to obtain employment, credit, insurance, security clearances, and other services and benefits. Not surprisingly, then, proposals to store a person's genetic information in a national network evoke several concerns about privacy.

Yet the Government and private sector regularly collect and "bank" personal information. The law enforcement community currently maintains databases that include much personal information, such as a person's name and aliases, fingerprints, criminal record, sex, eye and hair color, and some medical information, such as whether a person has epilepsy. Nevertheless, because DNA is specific to an individual and so highly personal, some are reluctant to see any DNA test results become part of a de facto national database. Still others fear that genetic testing will not be limited to identity, but will expand to include disease (e.g., sickle cell or Huntington's disease), proclivity toward disease (e.g., cancer or coronary disease), or behavioral characteristics (e.g., schizophrenia) that could then find their way into the database. Some believe it to be an inappropriate use of government authority to collect and store genetic information tied to a specific individual, because it is sensitive and personal. Related to these concerns are those about data security and the quality and reliability of the information that will be stored, should databanking of DNA results proceed.

One aspect of privacy considerations relevant to forensic applications of DNA tests can be separated into databanking DNA profiles v. storing DNA. Current proposals for law enforcement databases anticipate a need only for the test results of convicted offenders and unidentified crime scene evidence in investigatory databanks. Since the vast majority of tests are currently limited strictly to identification, such proposals assuage for many the privacy concerns of these types of databanks. For most people, the information most likely to be put, for now, into criminal history files-RFLP banding patterns for identification only—probably does not escalate privacy concerns because scientists do not currently know of any disease association with these markers. Contributing patterns of nondisease-linked DNA to military recruit files or newborn files might be indistinguishable from health status or a social security number for some.

Many object, however, to proposals for storing DNA profiles that can be associated with genetic disease, even though highly polymorphic areas of DNA correlated to disease exist and can be important in forensic casework. Further, many believe any type of DNA sample storage (as opposed to just coded DNA patterns) is inappropriate, primarily because it increases

the likelihood that there will be testing for information beyond unique identity. Still others believe actual storage of genetic material and information is included in that category of information-along with religion, votes, special confidences-that civil liberties tradition in this country protects from compelled disclosure.

Yet new means to detect and deter crime are necessary and compel great respect in this country. Violent crimes nationwide increased 5.5 percent from 1987 to 1988. With high rates of recidivism among convicted offenders, databases could be used to analyze whether evidence found at a crime scene matched a profile in the database, and thus provide police with a lead toward identifying a suspect. According to the Bureau of Justice Statistics, a survey of recidivism among State prisoners released in 1983 revealed that 62.5 percent had been rearrested within 3 years, with 41.4 percent returned to prison. Rearrest among violent offenders was 59.6 percent, and released murderers were about five times more likely than other offenders to be rearrested for homicide. In particular, the FBI believes DNA genetic databases will aid their efforts to solve some forcible rape cases—a woman is raped in the United States approximately every 6 minutes. Released rapists were 10.5 times more likely than other released offenders to be rearrested for rape. DNA genetic databanks could also be of aid to law enforcement in the growing number of serial crimes.

On the other hand, on a percentage basis, 6.6 percent of released murderers were rearrested for homicide and 7.7 percent of released rapists were arrested in new rape cases. Some opposed to DNA databases point out that many accused rapists choose to litigate only the issue of consent, thus the source of the semen—the only issue that can be addressed with DNA testing and databanks-is never in question. Research shows that blood evidence is 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 murder or rape only 5 percent of the time. These statistics appear less compelling than those presented by database advocates, and suggest a need to weigh potential social benefits of investigatory databases against both economic costs (expenditures to establish a databank) and, perhaps more importantly, potential social costs (including invasion of privacy.)

Finally, privacy considerations about forensic DNA analysis also center on DNA databases themselves—as opposed to whether to store DNA v. encoded DNA profiles. Civil liberties tradition holds that personal information collected under government authority should not be indiscriminately shared. The Privacy Act (U.S.C. 552a) offers some protection regarding data collection and access to information about most individuals included in Federal databases, but specifically provides that criminal justice agencies may exempt their record systems from many of its provisions.

If DNA information were to be incorporated into the NCIC Interstate Identification Index, as suggested by the FBI, access would be limited because noncriminal justice use is prohibited. The FBI has adopted privacy regulations that govern the NCIC. States that violate these standards can be denied NCIC services.

FBI proposals for DNA databases, however, envision maintenance **of DNA information in State criminal history files, which vary in their accessibility.** State law governs maintenance of non-Federal databases, and State criminal history files range from being completely open records, as in Florida, where private access is permitted, to being sealed from public scrutiny, as in Massachusetts. Concern about some types of criminal behavior, particularly sex offenses, 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). In addition, there has been increased

emphasis on such record checks for current and prospective Federal employees.

Informational privacy safeguards interests in personal freedom. 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, by whom, and the protocols for access to them. Recognition of these rights evinces a belief that individual freedom and liberty prosper when detailed information about a person's life is private. Ensuring that sensitive or stigmatizing information remains private protects an individual from harm.

DNA TYPING IN THE UNITED STATES: CURRENT PRACTICE AND FUTURE OUTLOOK

Despite the fact that only a few years have passed since DNA evidence was first used in a U.S. criminal proceeding and that several issues, such as technical standards, quality assurance, and civil liberties and privacy concerns, remain to be resolved, interest in implementing DNA typing at the Federal, State, and local levels has skyrocketed. Likewise, forensic applications of DNA analysis have generated excitement in the international law enforcement community (box l-D).

Commitment to forensic applications of DNA testing at the Federal level is demonstrated by extensive efforts by the FBI in research, training, technology transfer, and casework. With the mandated mission of performing research of value to both the FBI's DNA Analysis Unit and to State and local crime laboratories, the Bureau's Forensic Science Research and Training Center (FSRTC) has investigated applications of DNA typing to forensic casework since 1986, and has trained over 100 State and local forensic scientists in DNA techniques. Research at FSRTC encompasses a range of projects, including examining gel electrophoresis techniques that might replace current methods and evaluating environmental effects on reliability and validity of RFLP analysis applied to forensic specimens. In fiscal year 1989, FSRTC devoted approximately 20 percent ($104,200) of its research and training budget and 36 percent ($143,200) of its supply budget on DNA technologies. Seminars, symposia, the Visiting Scientist Program, collaborative research, and publications have been and continue to be important mechanisms used by the FBI to disseminate information about DNA techniques to State and local crime laboratories. Related to this role in technology transfer, as mentioned earlier in this chapter, the Bureau has served and continues to serve as a facilitator in discussions about many of the controversies surrounding forensic applications of DNA testing, including quality assurance, databanking, and statistical analysis and reporting of RFLP results.

In addition to these programs, the FBI Headquarters Laboratory established a DNA Analysis Unit to perform DNA tests on forensic samples from the State and local law enforcement communities at no cost to the jurisdiction. Since accepting casework in December 1988, and since reporting its first case in March 1989, the FBI DNA Analysis Unit received 2,619 samples for 536 cases as of July 1989; by mid-February 1990 these numbers had risen to 6,377 and 1,338, respectively. The FBI anticipates being capable of processing 10,000 samples per year.

DNA identification is a forensic tool that has been quickly embraced by the State and local criminal justice communities. Over three-quarters of 221 crime laboratories responding to a 1989 OTA survey stated that DNA typing is very important to their mission, and nearly one-half had contracted for this service with an outside facility (overall response rate of 85 percent). Forty-six percent of State and local crime laboratories said they have plans to implement onsite DNA testing in the next 1 to 2 years.

Yet costs associated with establishing and maintaining onsite capability will clearly be beyond reach of some crime laboratories (box l-E). The OTA survey revealed a diversity in

Box l-D—Uses of Forensic DNA Tests Internationally

An informal OTA survey in January 1989 of 40 countries found that at least 15 have implemented or are exploring forensic applications of DNA tests,[1] with most expecting to perform DNA typing of forensic samples in late 1989 or 1990. Two-the Republic of Korea and Yugoslavia—reported that such use of DNA identification was not planned. South Africa indicated that DNA typing is used only for medical applications at present, but embassy staff did not say whether this might be broadened to forensic uses. Yugoslavia also reported that such tests are used for medical applications.

The extent to which DNA typing technologies have been used abroad varies. In the United Kingdom, where forensic applications of DNA typing originated, single-locus and multilocus approaches have been fully accepted for criminal, paternity, and immigration casework. Over the past 2 years, Norway has gradually begun to use DNA typing in selected penal and civil cases. In other countries, DNA profiling is in an early, exploratory phase, with law enforcement units developing suitable systems and, in particular, collecting population data. In 1988, for example, Finland replaced traditional genetic human leukocyte antigen (HLA) typing for paternity cases with DNA-based profiling, which is now routinely used; DNA identification for criminal offenses has been used on a selective basis.

The Israeli police intend to use DNA typing on a routine basis, and as of February 1989 were beginning trials on case samples. The Main Office of the Polish police and the Polish Academy of Sciences are conducting research on DNA typing for forensic applications and anticipate field applications at the end of 1989 for selected rape and murder cases. Explorations into DNA typing for paternity purposes in Poland has been discontinued due to lack of funding. In the State of South Australia, RFLP analysis is used for paternity testing, and polymerase chain reaction has been used for crime work. Two of New Zealand's three forensic laboratories plan to be performing DNA analysis by early 1990. Several countries, while currently in the development phase, have contracted with commercial laboratories on a limited basis.

Full international cooperation that would result in standardization and a coordinated investigative databank as with some current NCIC files, appears beyond reach at the moment. On the one hand, close coordination between the Royal Canadian Mounted Police and the FBI will likely lead to effective data sharing from the outset-especially since the FBI anticipates its system eventually will become the de facto system in the United States. On the other hand, in anticipation of a unified European Community in 1992, officials of Denmark Italy, the Netherlands, the United Kingdom, and Federal Republic of Germany met and agreed to a series of issues pertinent to standardization, including a designated restriction enzyme (different from the U.S. system) and a common probe. Nevertheless, although current technologies and applications appear to have advanced too far for international standardization for the present, the situation is likely to change as future technical advances are adopted. In the interim, the Federal Government could facilitate dialogue and encourage cooperative efforts leading toward a system amenable to DNA identification among, not just within, international criminal justice entities.

---

[1] Australia, Canada, Finland, India, Ireland, Israel, Italy, Japan, New Zealand, Norway, Poland, Sweden, Switzerland, United Kingdom, and West Germany.

SOURCE: Office of Technology Assessment, 1990.

crime laboratory budgets and staff sizes, and further indicated that some might not even be able to cover costs of contracting with commercial laboratories for DNA typing (table 1-3)—13 percent of laboratories responding to the OTA survey have provisions to contract with private firms for DNA services, but may not be able to submit cases due to cost. Of the 110 laboratories contracting for tests, nearly half (49 percent) have not submitted budget provisions to do their own DNA analysis onsite. Thus, because it is not inconceivable that all forensic laboratories will reach a point where access to DNA typing will be essential, services provided at no cost by the FBI DNA Analysis Unit will become increasingly important. For laboratories pursuing onsite DNA typing services (41 have submitted budget provisions), some unique financing mechanisms are being employed, including revenue from a cigarette tax in one State and money derived from the sale of goods and property confiscated from drug-related investigations. At the time of the survey, only one laboratory conducted DNA identification onsite.

Box l-E—What Does DNA Typing Cost?

State and local laboratories have three options available to them if they are interested in DNA analysis of forensic specimens: the FBI DNA Analysis Unit, commercial laboratories, and onsite testing. The FBI laboratory provides DNA testing to State and local crime laboratories at no cost, while the fee structure of the three commercial laboratories varies from $200 to $490 per sample, or $1,500 per case, depending on the exact service and company (table 1-3). The FBI estimates that performing DNA typing on one sample, after a laboratory is equipped, will cost $28.50 (excluding labor), and ***$98.50*** including labor, but not overhead costs such as rent and utilities, which are included in the fee structures of the commercial companies. The Miami-Dade Police Department Crime Laboratory Bureau estimates it will cost their facility $41.60 per sample (excluding labor) and with labor costs added, $97.60. The cost of establishing a DNA typing unit onsite will vary from laboratory to laboratory, depending on the case load expected and existing equipment, but the FBI estimates that $60,000 to $70,000 would cover equipment expenses. Upto$11,000 more could be necessary to cover the cost of the FBI computer analysis hardware, and, should DNA databanking be implemented through the NCIC, States could expect an additional expense of approximately $200,000 for databanking efforts.

In addition to startup costs, a laboratory program would need to expect certain monthly operating costs. Although, again, the expense will depend on the number of samples on which a laboratory does DNA analysis, the FBI estimates monthly costs (excluding labor) based on handling 10,000 samples a year of approximately $18,100. The Miami-Dade facility estimates monthly costs (excluding labor) based on handling 3,600 samples a year of approximately $12,300. Future techniques are likely to rely increasingly on automation and could require a significant one-time outlay in exchange for greater speed and accuracy. Whether operating costs would increase or decrease with such automation, however, is difficult to predict.

Although the FBI provides DNA testing services at no cost, many laboratories will opt to do at least some DNA typing onsite. Enhanced turnaround time and the ability to keep evidentiary material are frequently cited as the primary benefits State and local facilities believe onsite DNA profiling will provide.

SOURCE: Office of Technology Assessment 1990.

Table 1-3—Costs for Forensic DNA Testing by Private Laboratories[a]

Service	Cellmark	Forensic Science Associates	Lifecodes
DNA testing	$490/sample	$1,500/case	$325/sample
Processing isolated DNA sample	$350/sample	Not available	$200/sample
Expert witness (daily rate + expenses)	$1 ,000/day (Ph. D.) $750/day (non-Ph.D.)	$100-$125/hr.	$750/day
Processing of insufficient sample	$21 O/sample	$250/sample	$125/sample

alnformation current as of June 1989.

SOURCE: OMce of Technology Assessment, 1990.

Overall, results from the OTA survey indicate that the likelihood of integration of DNA testing—via contracting or onsite—in the next 1 to 2 years appears mixed. Although 46 percent of labs have plans for onsite testing during this period, and 46 percent (not necessarily the same ones) have plans to contract with commercial laboratories, 21 percent stated they were not planning to contract in the next 24 months, and 51 percent have no plans for onsite testing. Fewer than 10 percent said they would neither contract nor had plans to pursue DNA typing onsite. Nevertheless, the demand from State and local crime laboratories for outside DNA profiling will likely continue in the future, since 83 laboratories estimated they will seek outside DNA analysis of from 2 to 3,000 samples.

Finally, the necessity for present and future cooperation between the FBI and State and local laboratories was clearly revealed by the OTA survey. Respondents believe, to varying extents, that an FBI role in many issues is appropriate (table 1-4).

Table 1-4-Suggested FBI Roles in DNA Testing

Question 4a: What role, if any, do you see for the FBI in DNA testing? (Please check all that apply).

Role	Percent of labs		
	Yes	No	No answer
Research (methods development and evaluation)	96[b]	2	2
Training	95	3	3
Casework for State and local labs	63	34	2
Maintenance of centralized DNA files	88	10	2
Reference library	77	20	3
Define standards	48	49	2
Certify laboratory personnel	24	73	2
Provide proficiency samples for quality assurance	55	43	2
Other	8	89	2

[a]The code number of the question in the survey instrument (see app. B.).
[b]Percentages may not add to 100 due to rounding.

SOURCE: Office of Technology Assessment, 1990.

THE ROLE OF CONGRESS AND POLICY ISSUES AND OPTIONS

With crime rates always a concern in local jurisdictions, the advent of any new method to assist investigators is welcomed. DNA testing has been no exception. Forensic applications of DNA tests have come to the attention of Congress because of the high visibility their use receives in congressional districts throughout the country. In fact, many Federal, State, and local law enforcement authorities have fueled public fascination in forensic uses of DNA tests by touting them as a revolutionary breakthrough in crime work, particularly rape and homicide cases. In some measure, congressional interest in recombinant DNA technologies, biotechnology, and the human genome project has also contributed to congressional interest in forensic DNA analysis.

Five policy issues related to forensic uses of DNA tests were identified during the course of this assessment. They are:

- quality assurance of forensic uses of DNA testing, including technical and operating standards for private and public facilities;
- funding of crime laboratories, forensic personnel training, and forensic research;
- the advisability of establishing computer databanks of DNA tests results;
- standardization of DNA analysis for improved data collection; and
- privacy considerations of collecting, using, and storing DNA data or samples.

Congress could play a role in each of these policy issues through oversight of activities related to forensic uses of DNA tests or through authorization of actions by the executive branch to set up formal coordinating structures or specific mandates—which could be freestanding or tied to appropriations.

Specific options that Congress could consider to address policy issues related to forensic uses of DNA typing build on the discussions presented earlier in this chapter and in chapters 3 through 6 of this report. Associated with each policy issue, discussed in turn in the following sections, are several options for congressional action that range from taking no specific steps to making major changes.

The order in which the options are presented does not imply their priority. Moreover, the options are not generally mutually exclusive: Adopting one does not necessarily disqualify others that pertain to the same or other issues, although changes in one area could have repercussions in others. A careful combination of options within and among the five policy issues could produce the most desirable effects.

Finally, since DNA testing is used in a criminal context, issues regarding the overall adequacy of the U.S. criminal justice system naturally arose during this study. Prominent among these issues was universal access to DNA typing for defendants, who often are less able than the prosecution to fund services. The adequacy of funding for defense-related services, however, is a broad social issue that is beyond the scope of this report. Nevertheless, access to DNA typing services and test results could be a topic tied to a number of the options presented for the five policy issues.

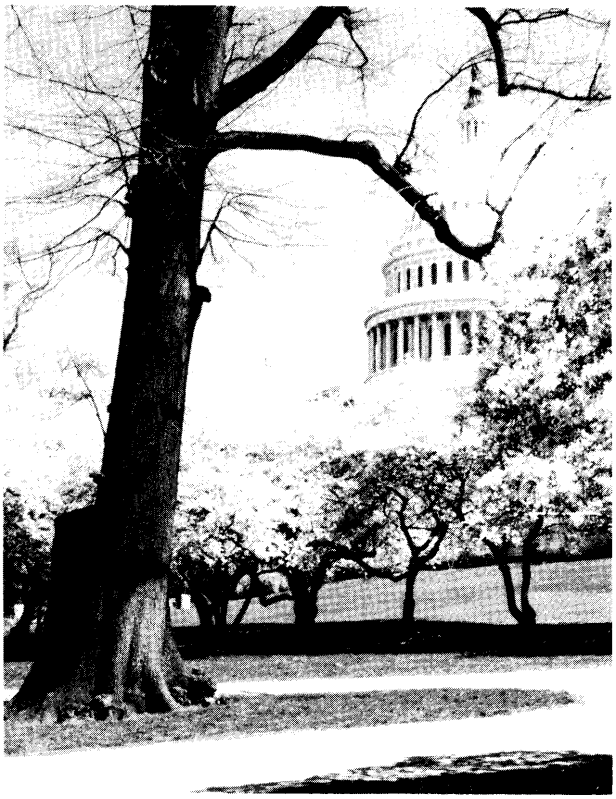


Photo credit: Robyn Nishimi

Quality Assurance and Standards

The issue of setting standards for forensic applications of DNA testing is the most pressing of the five policy issues identified by OTA. Standards for public and private facilities performing forensic DNA tests are essential to quality assurance of DNA analysis of forensic samples. Establishing standards at the earliest possible date is imperative.

OTA identified two distinct types of standards for forensic applications of DNA testing. Technical standards include matters such as proper scientific controls, choice of probe sequence, and analytic methods. Operational standards refer to areas of laboratory performance, such as recordkeeping, laboratory accreditation, licensing of personnel, and proficiency testing.

At present, neither the Federal Government nor any State regulates DNA testing by companies or crime laboratories. This situation is not unique to DNA analysis. Except in certain restricted areas, such as forensic alcohol analysis, no general licensing requirements for laboratories or personnel exist for crime laboratories. In contrast, Congress and the executive branch have stepped in to regulate drug testing laboratories and clinical laboratories.

Option 1: *Take no action.*

In the absence of congressional action to set or encourage adoption of technical standards, voluntary efforts by the FBI and professional organizations and case-by-case examination by the courts will likely move forward. FBI efforts to develop and disseminate recommended technical and operational requirements will continue. Continued case-by-case examination of proper technical and operational standards could slow full implementation of forensic analysis using DNA tests, as courts could become mired in scientific detail. If Congress takes no action, a haphazard array of standards could be developed, and disparate initiatives are likely to prove more expensive overall than a centralized effort. On the other hand, some feel the courts are adequately handling issues raised by the technology. By taking no action, Congress leaves to the courts the decision as to whether adequate technical and operational standards were employed in a particular case by a particular laboratory. In addition, if Congress takes no action, it would avert Federal oversight or regulation of the network of State and local crime laboratories that were established as local entities, which to date have been responsive only to their individual jurisdictions and are funded nearly totally by local monies.

Option 2: *Encourage the National Conference of Commissioners on Uniform State Laws to promote uniform practices in forensic applications of DNA tests.*

An organization set up for and by the States to promote uniformity of laws in a variety of areas, the Conference has Commissioners appointed by each State. In response to recommendations and appeals from numerous sources, it identifies areas where uniformity of law would

be useful, and drafts laws that are then proposed to State legislatures for enactment. For example, the Uniform Anatomical Gift Act was designed to address issues surrounding the area of organ transplant donation.

Congress could encourage the Conference—through a letter of request by a Committee or through legislation—to address the issue of standards and quality assurance for forensic DNA analysis. Adopting this option would signal congressional interest in uniform standards for forensic DNA typing, while leaving their development to a body controlled by the States. On the other hand, the Conference is under no obligation to respond to letters or legislation to address an issue, so the consequences could be the same as taking no action.

Option 3: *Encourage the use of a formal, open consensus review or conference to address and recommend quality assurance guidelines.*

Short of regulating forensic uses of DNA tests, Congress could facilitate voluntary efforts to achieve quality assurance of forensic services, including DNA analysis. Congress could specifically authorize the use of governmental agencies and appropriations to hold consensus conferences that would establish review processes or recommend protocols for technical and operational standards.

In encouraging this approach, Congress could exercise oversight to direct the FBI or NIST to hold consensus conferences and recommend procedures to ensure high-quality services for DNA analysis of forensic samples. A consensus process similar to that employed by the National Institutes of Health (NIH) could be effective and lead to greater quality assurance in forensic practices using DNA tests. An important consideration, however, is that the process should be open and represent the full range of stakeholders to be most effective, since many questions surrounding forensic uses of DNA technologies involve public policy decisions, not purely technical issues. Present efforts by the FBI to facilitate consensus-building fall short of an NIH-like process, because to date they have been meetings gathering a limited number of individuals by invitation.

Finally, Congress also could commission a private research institute or professional society to evaluate, through a consensus review process, quality assurance concerns pertinent to operational standards or technical standards. (In October 1989, a committee of the National Research Council, National Academy of Sciences, began a study of forensic DNA analysis—although not specifically to set standards—funded in part by the FBI and the National Institute of Justice (NIJ).)

Option 4: *Direct the National Institute of Standards and Technology of the Department of Commerce to review and report on acceptable technical standards for forensic applications of DNA tests.*

Identification of suitable technical standards by a neutral, nonregulatory agency whose mission is to conduct research in measurement standards would provide Federal oversight of setting technical standards and could enhance standardization of analyses, which could have a positive impact on databank initiatives (see following section). Directing NIST to report independently on technical standards might remove the objection of some to FBI-centered involvement in standard setting. On the other hand, because no regulatory authority exists for NIST, recommendations for appropriate standards would still be subject to voluntary compliance unless mandated otherwise by Congress. Voluntary compliance, including FBI participation, is likely to be perceived as less than sufficient by those who seek mandatory standards. A majority of laboratories, including the FBI laboratory, currently do not participate in the criminalistics accreditation program of the American Society for Crime Laboratory Directors.

Option 5: *Establish an independent commission to examine quality assurance issues surrounding forensic uses of DNA analysis.*

Congress could pass legislation to establish an independent commission to evaluate quality assurance issues of forensic DNA testing by Federal, State, local, and private laboratories. A commission directed to represent all interested parties could address either technical or operational standards (or both) necessary for quality assurance of forensic applications of DNA tests. As with directing NIST to examine technical standards, establishing an independent commission might remove the objection of some to FBI-centered efforts for both technical and operational standards. By the same token, absent a clear mechanism to implement any commission recommendations, some will view this option as insufficient. Furthermore, if Congress adopts this option, others will object to any effort to remove control of such issues from a laboratory-by-laboratory basis and will be concerned that an examination of general forensic laboratory practices would be imminent.

Option 6: *Enact broad-based quality assurance legislation that covers forensic laboratories.*

Congress could determine that current voluntary efforts to address quality assurance in forensic applications of DNA analysis, forensic practices in general, or both are insufficient or moving too slowly, and could enact broad-based quality assurance legislation that encompasses public and private facilities doing forensic casework. Legislation could be based, in whole or part, on similar, separate congressional action addressing regulation of clinical and drug testing laboratories. In the case of Public Law 100-578, which regulates clinical laboratories, Congress gave broad authority to an executive agency, but also specified detailed measures, including mandatory accreditation by Federal authorities or a private, nonprofit body meeting certain congressional criteria and approved by the Federal Government, national standards for certain laboratory methods, recordkeeping and reporting requirements, mandatory quarterly proficiency testing, sanctions, and penalties.

If Congress enacts quality assurance legislation, courts might be freed of some of the burden of having to evaluate certain aspects of DNA testing, or other forensic scientific analyses—although the onus would remain with the laboratory to demonstrate it had adhered to good laboratory practices. Establishing legislatively mandated responsibility would likely satisfy those individuals who believe Federal oversight and regulation of public and private laboratories doing DNA analysis specifically, or forensic casework generally, is necessary. On the other hand, although States do not currently regulate their own laboratories, local crime laboratories, or private laboratories accepting forensic casework, they likely will object to Federal preemption of their authority to regulate their facilities—regardless of whether such regulation pertains only to DNA tests or includes other technologies.

Congress could enact quality assurance legislation that encompasses only private laboratories, and could require States to implement measures for State and local laboratories. Such legislation could mitigate some objection to Federal intervention, but is likely to be opposed by the few private companies that exist and by those who believe a Federal regulatory role is needed for all forensic laboratories doing forensic casework.

Option 7: *Direct the U.S. Attorney General to set and oversee technical and operational requirements for forensic uses of DNA testing.*

Present efforts by the FBI on behalf of the U.S. Department of Justice focus on facilitating the development of laboratory standards. Congress could decide that direct Federal regulation and oversight is necessary, and enact legislation directing the U.S. Attorney General to implement standards for forensic uses of DNA typing and to ensure compliance. Mandatory Federal standards at both the technical and operational levels could be issued, while allowing the U.S. Attorney General flexibility in how such stan-

dards would be set, evaluated, and refined as DNA typing technologies advance. For example, Congress could direct the Attorney General to adopt a process similar to the NIH Recombinant DNA Advisory Committee, which has demonstrated how a flexible Federal role to oversee recombinant DNA activities can evolve.

Nevertheless, placing the U.S. Attorney General or a designee such as the FBI in the role of regulator is likely to receive strong opposition from both State and local crime laboratories as well as other interested parties. Fewer than half the laboratories (48 percent) surveyed by OTA believed setting standards was an appropriate role for the FBI. Only 24 percent believed providing certification was appropriate. State and local facilities are likely to resent intrusion of Federal authority in what has been, to date, locally funded and operated entities. Others not connected to crime laboratories probably will object to FBI oversight as a situation of the fox guarding the hen house. ' Finally, it is likely that the FBI will prefer to retain its role as an investigative agency, rather than a regulatory body. Further, because regulatory duties would require a significant sum of money for development and enforcement of standards, appropriation of new funds or reallocation of existing Department of Justice funds would be necessary if Congress adopts this option.

Funding for Forensic Sciences

Hand-in-hand with standards for forensic DNA analysis is ensuring that education and training of personnel is adequate, that facilities are properly equipped and funded, and that basic research to evaluate forensic applications of DNA be performed. Most agree that crime laboratories and forensic sciences research that supports technology transfer to crime laboratories are underfunded. Increasingly, indications are that crime laboratories are experiencing difficulties managing the steadily rising influx of casework. Interest in implementing DNA testing onsite, which could be coupled to increased requirements for laboratory accreditation, personnel licensing, or proficiency testing, is likely to further stretch fiscal resources and exacerbate the casework backlog.

Crime laboratories are public facilities that receive operating monies from State, city, and county sources, with little direct Federal investment. Present Federal spending is largely indirect, taking the form of research, training, and casework. Is State and local funding of crime laboratories sufficient, or is additional Federal assistance necessary?

Option 1: *Take no action.*

Congress could conclude that State and local funding for crime laboratories is adequate. If Congress takes no action, State and local governments will continue to fund crime laboratories through a variety of mechanisms. Laboratories planning to conduct DNA typing onsite will need to make substantial investments of funds and personnel. A push by law enforcement, prosecutors, defense attorneys, and politicians for widespread dissemination of DNA typing in crime laboratories without attendant increases in funds would place additional financial burdens on facilities already strapped for personnel and money. Additionally, if Congress takes action to implement standards such as licensing or proficiency testing, or to standardize DNA analysis of forensic samples to enhance databanking efforts, and takes no action to provide increased Federal assistance, State and local funds to cover costs associated with such actions will need to increase or be diverted from other crime laboratory activities.

For State and local crime laboratories that cannot conduct DNA testing onsite, the FBI will continue to accept their casework. If Congress takes no action and State and local resources prove limited, however, the number of crime laboratories relying on the FBI for DNA testing of forensic samples will likely increase and could strain resources the FBI has devoted to its DNA analysis program.

Option 2: *Increase direct Federal support for crime laboratories.*

Federal funds support crime laboratories indirectly through research and training at the FSRTC and casework performed at the FBI's forensic laboratory, and DNA typing is one of the array of forensic tools supported by these efforts. Only a minute fraction, however, of Federal funds for crime laboratories is direct. The lack of available funding for some crime laboratories to implement DNA testing highlights a much larger issue: that of insufficient funding and personnel for crime laboratories to carry out even routine forensic science procedures, let alone DNA analysis.

Congress could conclude that State and local crime laboratories need additional funding to perform their missions effectively, and could directly appropriate funds for distribution to these facilities; such funds could be linked to quality assurance and standards requirements. Congress could designate that the funds be slated solely to support DNA testing, or could leave the nature of programmatic spending to State or local discretion. Congress also could require that funds be matched by State and local monies. Increased general Federal support, not tied to DNA typing, might provide the best relief for laboratories with casework backlogs. Providing directly for DNA testing could release additional State and local funds for other forensic analyses or personnel training, but it also might result in no net gain in crime laboratory funds if State or local monies designated for forensic serology and DNA analysis were diverted from crime laboratory budgets rather than used to supplement other crime laboratory activities. Such a situation, while allowing State and local laboratories to perform DNA tests on forensic samples, would not alleviate, for example, case loads in firearms or drug analyses. Present budgetary concerns also would need to be balanced against the need for Federal spending in this area.

Option 3: *Increase Federal support for the training and education of crime laboratory personnel.*

Federal funds, chiefly through the FBI and to a lesser extent through NIJ, support training and education for active and future crime laboratory personnel. For example, FSRTC provides training to crime laboratory analysts in numerous areas, including biochemistry, physics, polygraphs, latent fingerprints, toxicology, immunology, and DNA analysis.

Given the rapid pace of scientific and technical developments in forensic casework, Congress could decide to increase funding for training and continuing education of crime laboratory personnel. Congress could focus on funding courses specific to applications of DNA typing, or could appropriate training and education funds on a broad basis. In increasing Federal support, Congress could appropriate increased funds to the FBI for training at FSRTC, to NIJ for grants to academic institutions to train future forensic analysts or to hold continuing education courses, or directly to State and local laboratories to offset costs of training personnel. For example, Congress could provide increased funding that would allow FSRTC to hold more DNA testing courses, which are currently oversubscribed. Nontargeted training grants through NIJ or directly to crime laboratories could encourage the development of programs tailored to specific needs of State and local facilities.

Option 4: *Increase Federal support for basic research in forensic applications of DNA technologies.*

Federal funding of research specifically in forensic applications of DNA analysis is limited. Congress could encourage the transfer to crime laboratories of state-of-the-art molecular genetics techniques developed in basic biomedical research laboratories by increasing support for "bridge" research in forensic applications of DNA techniques—i.e., research that explicitly evaluates new molecular techniques applied

to forensic specimens. Such bridge research strengthens the underlying scientific and technical knowledge base for DNA analysis of forensic casework.

Congress could increase support by directing monies to FSRTC, to NIJ for grants to academic departments, or to both. If Congress increases Federal appropriations for such research, present controversies surrounding technical standards for forensic applications of DNA technologies might be more quickly resolved, or perhaps even avoided, as additional techniques are adopted by crime laboratories. In an era of fiscal constraint, however, increased Federal spending for basic research in forensic applications of DNA technologies would need to be evaluated against the backdrop of Federal budget considerations.

Advisability of a Databank

The FBI and others in the criminal justice community believe that realization of the full law enforcement potential of DNA testing depends on developing investigative databanks of DNA patterns that are accessible nationwide. Proponents of such databanks often cite high rates of recidivism among violent offenders and the growing incidence of serial crimes as justification for electronic storage of genetic profiles. Many experts who recognize the importance of a nationwide databank oppose investigative DNA databanking for the moment on technical grounds, arguing that such proposals are premature given the great technological flux likely to occur in the near future. And although current databanking proposals recognize the need to incorporate flexibility in their design so that files can be updated as technologies improve, predicting the course of forensic DNA analysis to account for changes even over the next year or two could prove tricky; accurate long-term forecasting of the precise direction is impossible. Finally, others oppose DNA computer databanks on the grounds that the purported benefits fail to outweigh the threats to civil liberties they pose.

The FBI has developed computer hardware and software necessary to convert DNA testing results to data amenable to computerized storage and retrieval. These tools will be provided to all users of their testing system. Along with others, it is discussing a proposal to implement a nationwide investigative DNA databank network. Additionally, the FBI maintains a computer network, the NCIC, that provides for swift exchange of electronic information between criminal justice organizations at the Federal, State, and local levels. The Director of the FBI has committed himself to including DNA testing results in NCIC files.

Commercial laboratories, State and local laboratories, and the FBI have already established databases of population statistics to support their RFLP analysis systems. Collecting population data information for noninvestigative purposes enhances the population genetics knowledge base necessary to refine statistical analyses of forensic applications of DNA typing. Such DNA databanks are not controversial, for the most part, and so limits on such DNA databanks are not discussed.

Option 1: *Take no action.*

Computerized DNA information could benefit criminal investigative work via three classes of files: *open cases* (where a suspect has not yet been identified), *known offenders* (most likely rapists and murderers), and *missing/unidentified deceased persons.* Several States have passed or proposed legislation that would support establishment of known offenders' files, by requiring DNA typing results on certain convicted offenders (most often defined as sex offenders or violent offenders). No State has actually begun investigative databanking at this time, but sample collection is under way or imminent in several locales. If Congress takes no action, the FBI will likely proceed with plans to create several investigatory databases containing DNA profiles (most likely in the NCIC) and to integrate these files with State and local efforts that adopt the FBI DNA analysis protocol.

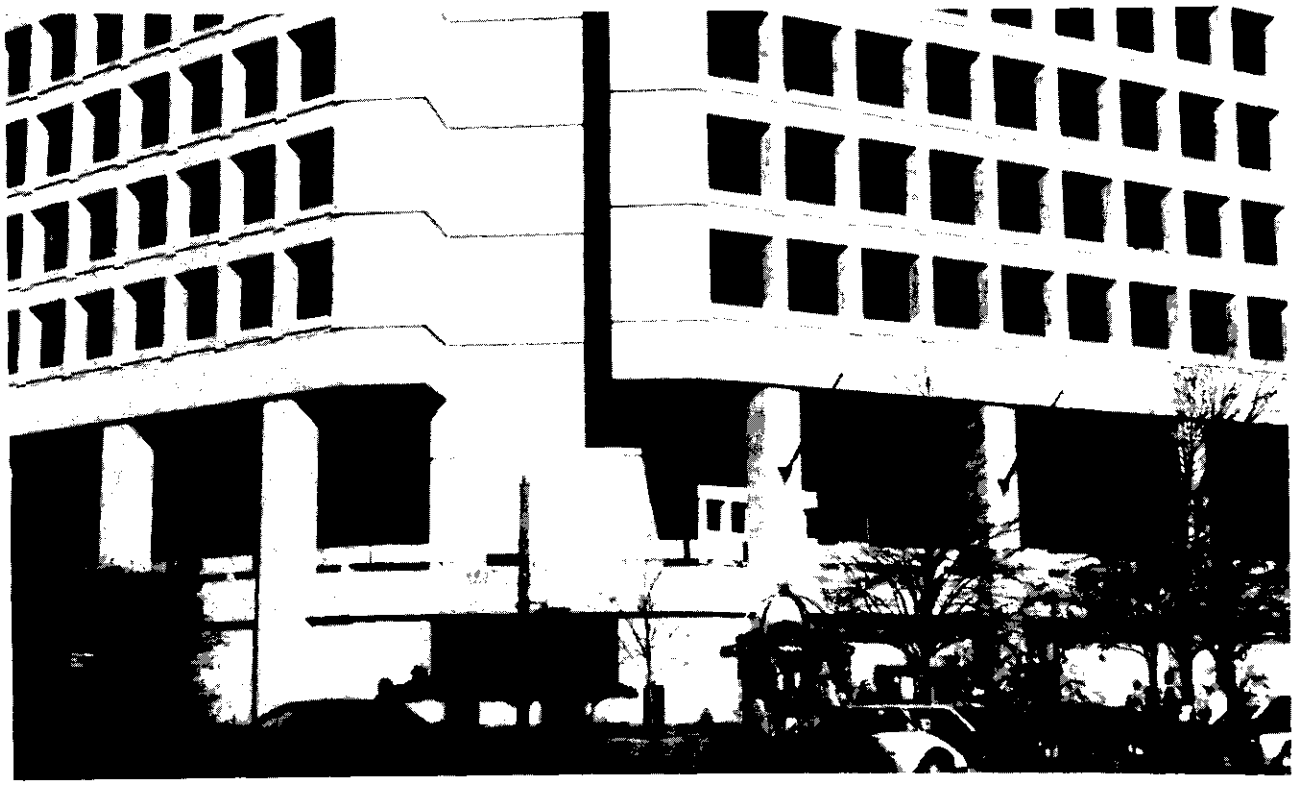


Photo credit: Kevin O'Connor

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

Option 2: *Place limits on interstate DNA databanking activities.*

If technological and social considerations appear to need further exploration, Congress could enact legislation to place limits on all law enforcement activities related to interstate electronic transmission of DNA test results, could prohibit FBI activity in the area of database development or interstate transmission of DNA information, or both. Such legislation could be for a limited or an indefinite period, and could be targeted to investigative databases, population frequency databases, or both.

Adopting a short-term moratorium on *any* interstate DNA databanking analysis could mollify some concerned about technological considerations and privacy, but it would limit the FBI and local agencies in their mandate to fight crime. Enacting legislation that limits all interstate electronic activities related to DNA typing would be viewed by many as draconian, although it would be applauded by some concerned about privacy considerations. Limits or a ban on interstate transmission of DNA test results would not prohibit a State from storing DNA test results for crimes within its border, but cooperation with a neighboring State, for example, via a computer network of DNA results would be precluded.

Because population frequency databanking is largely uncontroversial from both the privacy and technological perspectives, as well as being considered necessary to improve and refine reporting of forensic DNA test results, legislation suspending interstate or FBI databanking activities related to population frequency activities would likely cripple forensic DNA analysis nationwide.

A moratorium directed solely toward the FBI's nationwide investigative DNA databank could allow time for a full public discussion of important issues, not only those pertinent to

privacy but also technology-related considerations, including those involving standardization (see following section). But it might also be viewed as an unnecessary delay because the FBI plans to store just DNA profiles involving its system, which currently involves only noncoding, nondisease-linked DNA. A prohibition on FBI activities in this area would deny the law enforcement community the opportunity to implement what it sees as the one of the chief utilities of DNA typing and a computerized network of profiles: the ability to link an unknown biological sample from a crime scene to a specific individual.

Although legislation that specifically precludes FBI investigative databanking efforts might not limit State efforts per se, if States had to provide the telecommunication and, especially, the indexing capabilities necessary for interstate transmission of test results, the costs of the system could outweigh the perceived benefits. Further, absent the FBI, there would be no clear coordinator of interstate database activities—for prototype development or implementation. It is unlikely that the States could successfully implement an investigative DNA databank without Federal support. Thus, adopting this option would at some level hinder DNA analysis as an investigative tool of law enforcement and effectively eliminate its utility for cross-jurisdictional purposes.

Option 3: *Encourage Federal and State DNA databanking activities.*

Congress could directly encourage DNA databanking by appropriating funds to the Department of Justice, State and local governments, or both. Such funds could be for investigative datafiles or for improved data collection on population frequency information related to DNA typing. The Federal Government, through efforts of the FBI, has an interest in collecting broad-based information to ensure accurate population frequency data for RFLP analysis of forensic samples. Congress could direct funds to State and local laboratories doing DNA typing that would facilitate the collection and transfer of individual laboratories' genetic population frequencies to the FBI or its designee. Improved population genetics data enhances DNA analysis of forensic samples. Further, FBI implementation of a national investigative DNA profile databank would benefit from close coordination with States in gathering this information. Encouraging immediate implementation of electronic storage and transmission of DNA typing results for investigative purposes would be opposed by many—on privacy and technical grounds— and would require concurrent examination of two other policy issues: standardization for databanking and privacy considerations.

Standardization for Databanking

Whether or not Congress takes action to intervene in database development for forensic uses of DNA analysis, the issue of standardization could warrant attention. Standardization is an issue distinct from setting standards to achieve quality services. It involves developing a uniform, national system of certain techniques to make DNA analyses compatible for exchange through computer data systems across the 50 States. An effective, nationwide database will depend on standardization and quality control of both the test and the computer technologies necessary to extract and transmit DNA information. Without standardization, the potential for databanking will be limited unless each organization conducting DNA tests collects the same type of information. Devising an institutional means to settle on standardized data is generally agreed as critical to a successful national DNA databank, although a few would argue that methods could possibly be developed to apply conversion factors to data not obtained through the standardized protocol. Thus, the issue is whether the Federal Government should promote standardization of DNA testing to improve data collection, which would make DNA databanking further amenable for investigative use.

Option 1: *Take no action.*

Several factors currently operate to encourage standardization even in the absence of congres-

sional action. Because of the high interest in establishing a network of DNA profiles for investigative purposes, the incentive is high to standardize. Still, of the two crime laboratories doing onsite DNA testing as of August 1989, one had adopted the Lifecodes methodology, but the other was switching from Lifecodes' to the FBI system.

If Congress takes no action, it is likely that the current FBI system and future refinements of it will become the de facto system in the United States. Several organizations favor adopting the FBI's testing system so that a national DNA profile databank can be achieved. Furthermore, the FBI also provides two services that encourage standardization using their system: They currently conduct tests on State and local specimens at no charge, and they offer free training in their testing methods for State and local laboratories who choose to establish DNA testing capability onsite.

Option 2: *Appropriate funds for States contingent on adoption of standardized technology.*

Congress frequently uses incentives to encourage certain results from States. Congress could allocate funds to speed the penetration of DNA testing and databanking throughout the country, could tie such grants to quality assurance, and could make those funds available only to States or localities that agreed to use them for specific types of testing materials and computer hardware and software. This action would both encourage the quality and standardization necessary for successful databanking and provide Federal funds for forensic uses of DNA typing in jurisdictions perhaps otherwise unable to afford it. It might also have the effect, however, of locking States into a testing technology that could soon become outdated, and could be viewed as micromanagement of State criminal justice affairs. This effect might be mitigated by delegating to the FBI the authority to regulate standardization of the initial technology selection and future alterations, rather than standardizing DNA forensic analysis through legislation.

Option 3: *Direct the FBI to deny NCIC access to States that fail to implement a technology according to a standardized protocol.*

Since NCIC exists by legislative authority, Congress could enact legislation specifying the terms by which its services are made available to the States. Depending on the perceived importance of DNA testing to criminal justice, total or partial access to NCIC could be predicated on compliance with standardization. At one extreme, Congress could direct the FBI to deny access to all NCIC files, including fingerprint, vehicles, or other files, to any State that fails to comply with federally directed DNA standardization. Or Congress could direct the FBI to construct NCIC files to hold only standardized information and make no provisions for handling nonstandardized data. Such an action would deny the use of DNA files to States that fail to standardize, while allowing them to have continued access to other NCIC files.

Privacy Considerations

Civil liberties and privacy considerations are important policy issues often raised separately in the context of genetic information or computer technologies. Forensic applications of DNA typing involve both. Although the question of standards for forensic DNA analysis is the most pressing issue in this field, policy decisions by Congress and the executive branch on privacy considerations loom and are likely to be more controversial.

Citing the inherent intimacy of genetic information, the current and developing ability to test for personal information other than unique identity, and the difficulties of maintaining confidentiality in a computer network, experts raise concerns that genetic information could be used unfairly to deny future benefits to persons with criminal records, and that genetic profiling within the criminal justice sphere could lead to wider testing and broader threats to privacy. And the probability that DNA will be stored in some form, in addition to test results, heightens concern about an increased likelihood that

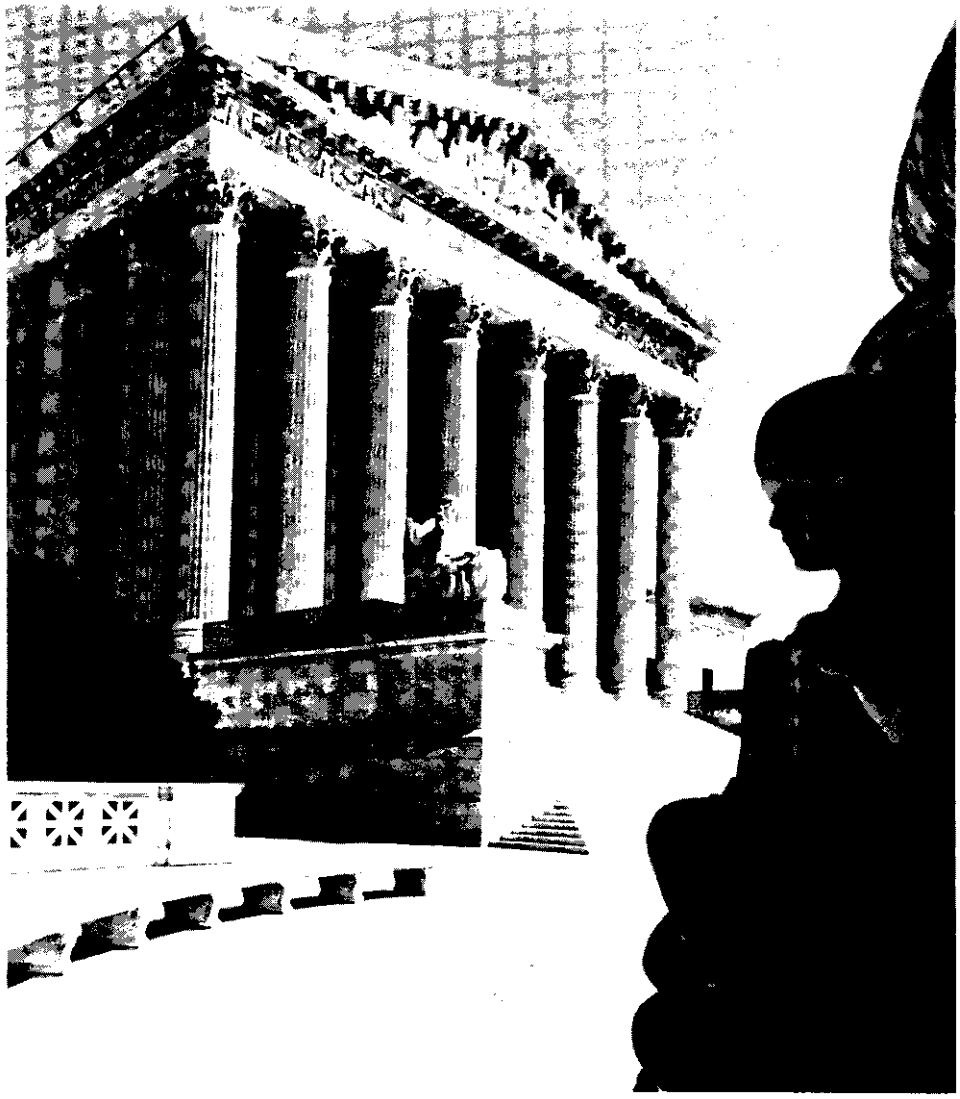


Photo credit: Jake McGuire, Alexandria, VA

stored DNA will eventually be probed for genetic information beyond identity.

Option 1: *Take no action.*

By taking no action, Congress delegates to the FBI and State and local governments several civil liberties decisions: Specifically, the appropriate level of privacy protection to be afforded the collection, use, and storage of DNA data or samples. Since existing privacy laws and regulations among these jurisdictions differ widely, their application to DNA records will span the range of privacy that States currently provide for other types of criminal records—from closely held within the criminal justice community to freely available to the public. State laws passed and proposed to collect material for DNA typing from individuals and to store samples, results, or both also would continue and will vary from jurisdiction to jurisdiction.

Option 2: *Establish a commission to study the privacy considerations related to collection, use, and storage of genetic information and material.*

The specter of a de facto, widely accessible national database indexed by a genetic identifier and containing personal genetic information

attends most proposals for genetic databanking, whether the proposal addresses forensic applications of DNA tests, medical diagnostics, or efforts to map the human genome. Concerns raised about genetic databases evolve from a strong tradition of protecting individual liberty and compete with arguments supporting the utility of genetic databanking. Congress could establish a commission to study the broader social implications of DNA databanking. Since only preliminary steps have been taken to establish genetic databanks within the law enforcement community, a study of these competing concerns, which could be designed to merely clarify the issues or to try to reach consensus on them, could be a timely and useful addition to the debate. A commission charged with examining privacy considerations of collecting, using, and storing genetic information could also evaluate privacy issues about DNA testing proposed beyond criminal justice applications, including, for example, typing military personnel or DNA typing as a tool for missing children.

By taking a lead in fostering discussion about these issues, Congress could preempt some criticism that DNA databanking proceeded without adequate consultation of the public. Unless the commission acted in a timely manner, however, Federal and State endeavors would continue unabated. And, depending on the outcome of the commission's work, State efforts and conclusions could be preempted.

Option 3: *Allow DNA test results to be databanked, but prohibit storage of DNA.*

One particularly acute civil liberties concern is that current and future DNA-based tests for genetic diseases and predispositions will be used on forensic samples and their results stored in Federal or State computer databases. In particular, the probability that DNA samples will be stored in addition to test results heightens concern about the increased likelihood that stored DNA samples will eventually be probed for genetic information beyond identity. Congress could enact legislation that expressly allows only planned FBI efforts to databank RFLP patterns for identification purposes to proceed, but that limits from whom samples can be taken for analysis and prohibits DNA sample storage by the FBI and other forensic facilities.

Such legislation could be perceived by many as a step to ensure that personal genetic information beyond DNA profiles does not find its way into centralized computer data files that could have adverse effects on an individual's future, including employability or insurability. Scientific and technological developments in molecular biology and genetics, including efforts to map and sequence the human genome, are proceeding rapidly, however. Prohibiting law enforcement officials from storing DNA would preclude them from applying new technologies or probes to reprofile individuals with state-of-the-art methods. Further, crime scene samples are presently retained by each jurisdiction until their value as evidence no longer exists. Because today's technology allows near-permanent storage of some types of suspect or victim evidence, distinguishing between storing actual DNA and storing evidence containing DNA is impossible. Thus, Congress might need to consider a timeframe beyond which evidence samples could not be stored, which could hamper criminal investigations. Finally, restricting DNA storage could result in a databank of information locked into a dinosaur technology, or one with varying profiles depending on when an analysis was performed.

Option 4: *Limit the type of genetic information that can be stored in federally supported systems.*

Opponents of DNA databanking frequently cite the ability of DNA tests to reveal more than unique identity-e. g., genetic conditions, predisposition to diseases, or, in the future, behavior characteristics—as a primary reason for their objections. They fear that identity testing could lead to full probing of an individual's DNA samples, with subsequent storage of sensitive, medically informative details in databanks that

cannot or will not be protected from unauthorized access.

Congress could enact legislation to prohibit the FBI from supporting storage or transmission of the results of DNA tests that probe anything other than portions of the human genome that are both noncoding and not associated with disease genes. (Both criteria, because many noncoding, ''junk' regions of DNA can be medically informative). Racial or ethnic identifiers could remain in the system, if Congress deems such distinctions as important for population statistics or other purposes. Details that could be precluded as DNA probes become available range from health factors to eye color.

Legislation that specifically precluded the FBI or any Federal entity from participating in the interjurisdictional transmission of results of DNA tests for anything other than noncoding, medically uninformative DNA might assuage the fears of some. Currently, the FBI uses only DNA analyses that test nondisease-linked DNA, thus such legislation would have no ill effect on the FBI's intentions to employ DNA databanks as investigatory tools. If Congress adopts this option, it would also limit the utility of storing DNA samples except to the degree that they were saved to accommodate technical advances in identity testing. On the other hand, limiting information only to noncoding DNA patterns could hinder law enforcement efforts as scientists elucidate genetic details such as eye color or hair color. Confining electronic storage to just "junk" DNA also would prevent the use of many well-characterized and highly polymorphic genetic markers that are not noncoding sequences, but that could be of significant use in forensic DNA analysis.

Option 5: *Place more stringent restrictions on access to genetic information stored in federally supported databanks.*

The Freedom of Information Act does not compel the FBI to release sensitive personal information contained in criminal history files, but neither does the Privacy Act compel the FBI to keep such information confidential. The FBI has adopted regulations to protect the privacy of criminal history information, but compliance with these regulations is largely voluntary. In recent years, Congress has authorized Federal cooperation with criminal history checks on potential employees in several fields. The combined effect of existing law is to make it possible, if not likely, for employers, insurers, and noncriminal-justice government agencies to gain access to genetic information of persons with criminal records if such information is contained in the NCIC.

To ensure that information collected by the law enforcement community is used solely for intended uses, i.e., criminal justice identification or investigations, Congress could prohibit dissemination of genetic information stored in federally supported databanks outside the law enforcement community. Congress also could prohibit private contractors from possessing such data, and, in addition, could enact legislation to require the FBI to place special restrictions on access to genetic information and include sanctions for noncompliance-e. g., denying NCIC access to States that fail to abide by the guidelines for protection of genetic information. Singling out genetic information for specific limitations on dissemination would indicate that Congress believes genetic data to be special, requiring new or extended protection if placed in computer databanks. Adopting this option, however, would likely be viewed by some as unduly burdensome intervention in an area where adequate protection and restriction exists.