
The Expanding Use of DNA in Law Enforcement: What Role for Privacy?

*Mark A. Rothstein and
Meghan K. Talbott*

DNA identification methods are such an established part of our law enforcement and criminal justice systems it is hard to believe that the technologies were developed as recently as the mid-1980s, and that the databases of law enforcement profiles were established in the 1990s. Although the first databases were limited to the DNA profiles of convicted rapists and murderers, the success of these databases in solving violent crimes provided the impetus for Congress and state legislatures to expand the scope of the databases with little critical examination of each expansion's value to law enforcement or cost to privacy and civil liberties.

We are now entering a new stage of DNA forensics, in which successive database expansions over the last decade have raised the possibility of creating a population-wide repository. In addition, new applications of DNA profiling, including familial and low stringency searches, have been added to DNA dragnets, the use of medical samples for forensic analysis, and other measures to create a series of crucial, yet largely unexplored, second-generation legal and policy issues. In this article, we assess these emerging issues and conclude that limits must be placed on the use of DNA in law enforcement and that privacy considerations must play an important part in the development of policies for the use of DNA profiling.

The Expanding Use of DNA

Scope

State DNA databases, which began almost exclusively as collections of adult sexual offenders' DNA profiles, have now expanded to include many or all convicted felons, juvenile offenders, those convicted of certain misdemeanors, and even arrestees.¹ In 2004, California voters approved Proposition 69, expanding the state database of felons convicted of serious, violent crimes, to include samples from *all* felons and individuals with past felony convictions. The state will expand its database in the future to include profiles from individuals arrested for felonies and even individuals detained as mere suspects.² Laws in Louisiana,³ Texas,⁴ and Virginia⁵ also authorize collecting DNA samples from arrestees. Recently, the DNA Fingerprinting Act

Mark A. Rothstein, J.D., is the Herbert F. Boehl Chair of Law and Medicine and Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. He received his B.A. from the University of Pittsburgh and his J.D. from Georgetown University.

Meghan K. Talbott, J.D., is a Research Associate at the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. She received her B.A. from Stanford University and her J.D. from the University of Louisville.

There is virtually no scientific, comprehensive, independent, peer-reviewed analysis quantifying the overall effectiveness of DNA databases in solving or preventing crimes.

of 2005 was signed into law, authorizing the expansion of the federal DNA database to include DNA collected from “individuals arrested, and from non-United States persons who are detained under the authority of the United States.”⁶

The prevailing view among law enforcement officials is that more profiles included in a database allow a greater chance that a profile will match evidence found at a crime scene.⁷ The promise of increased efficacy has some members of law enforcement and legal academia advocating for the expansion of criminal DNA databases to include DNA samples from the entire population.⁸ Proponents of expansion argue that reducing the social cost of crime justifies the creation of a population-wide database, and that a universal database is necessary to maximize the utility of DNA profiling.⁹ Although a few countries, such as Iceland and Estonia, are establishing national DNA databases for research purposes,¹⁰ no country has implemented a population-wide database for forensic purposes.¹¹ Yet such an endeavor may not be far off. In 2005, the Portuguese government announced its intention to create a DNA database including the DNA profiles of all its approximately ten million inhabitants.¹²

A variety of practical and policy issues need to be addressed before a population-wide DNA forensic database can be seriously considered in the United States. On the practical side, virtually every state reports a substantial backlog in the analysis of extant samples collected under current laws, including crime scene evidence.¹³ There are too few trained laboratorians, and nearly all states lack the equipment and storage facilities to support a major increase in the scope of the databases. Cost is also an issue. At a time of budgetary constraints, new DNA forensic expenses would likely consume a substantial percentage of new funds that could be allocated to law enforcement.¹⁴ It is an open question whether the cost of a database expansion would deter crime and thus justify foregoing expenditures for additional front-line personnel, other forensic equipment, new vehicles, weapons and protective equipment, or crime control programs.

Assuming that the practical issues can be overcome, we are left with the policy question concerning whether we ought to develop a universal database. Notwithstanding civil liberties issues (discussed below), it is essential to have a clear picture of the expected law enforcement benefits. To justify a database expansion, even from a purely financial standpoint, there must be

convincing evidence of the likelihood that databases of increased scope would be significantly more effective than the current databases in solving and preventing crimes in absolute terms and relative to other possible law enforcement expenditures. What is the evidence?

The Combined DNA Index System (CODIS), started by the Federal Bureau of Investigation (FBI) as a pilot program in 1990, was formally established in 1994.¹⁵ Through its tiered system of databases, CODIS enables federal, state, and local crime laboratories to exchange and compare DNA profiles electronically, thereby linking crimes to each other and to convicted offenders. Over a decade of experience with DNA databases in most states supports the following two conclusions. First, DNA databases have had many spectacular successes in connecting seemingly disparate crimes and in identifying probable perpetrators in the absence of any other leads. Second, including “lesser offenses” in the databases helps to solve an indeterminate number of later, more serious crimes. For instance, yesterday’s burglar may be today’s rapist,¹⁶ and having the DNA from a previously convicted burglar may help in solving a subsequent rape case.

Although recognizing these points, we note that there is virtually no scientific, comprehensive, independent, peer-reviewed analysis quantifying the overall effectiveness of DNA databases in solving or preventing crimes. The only quantitative measure used to assess the value of DNA databases is the total number of “cold hits” or “investigations aided.”¹⁷ These totals make for good headlines and legislative testimony, but their use raises a number of serious methodological and policy concerns. To begin with, there is no clear definition of the terms “cold hits” or “investigations aided,” and thus the inclusion criteria vary widely among jurisdictions or even individual reporters. There is also no comparative information available to estimate the likelihood that other forensic techniques or additional investigation would have identified the suspect.

It is also not clear how many of the “investigations aided” actually result in conviction. Based on the claims of increased efficacy in solving crimes, one might expect that the percentage of crimes being solved or “cleared” would have increased as DNA databases expanded. However, while the crime rate has dropped over the past ten years, clearance rates have changed very little during that period. Moreover, the clearance rates for crimes typically associated with the availability of perpetrator DNA, homicide and forcible rape,

were actually lower in 2004 than in 1995, meaning that law enforcement actually solved fewer of the reported crimes than it did when DNA databases were still in their infancy.¹⁸

A match between crime scene DNA and an individual's database profile does not necessarily mean that the individual is guilty. For example, a murder suspect might have acted in self-defense or there may be some other reason to account for the presence of DNA found at the crime scene. Indeed, according to one study in Virginia, DNA matches resulted in convictions in less than thirty percent of the cases.¹⁹ Case resolution, not conviction, may be a more accurate measure of the effectiveness of DNA databases. For example, a suspect identified by DNA may have subsequently died without a conviction, yet in another case, a single DNA match may lead to multiple convictions where a suspect identified by his or her DNA confesses to other crimes without DNA evidence.

Finally, virtually all of the data are compiled and released by crime laboratories and other entities with an interest in promoting the maintenance or expansion of DNA databases. Unfortunately, a series of scandals throughout the country in which DNA evidence has been negligently (and even worse, intentionally) misidentified,²⁰ must give one pause before accepting at face value any claims by interested parties about the effectiveness of the DNA forensic identification system. In the absence of rigorous, independent, scientific studies of the efficacy of DNA databases of varied scope in helping to solve a range of crimes, it is foolish to consider further expansion of the current system.

Even without adequate data, it is still possible to compare, from a policy standpoint, today's typical state DNA database (restricted to most or all felons) with a universal database. The two compelling justifications for establishing a forensic DNA database of sex offenders, violent felons, or all felons is that these individuals are likely to engage in repeated criminal activity, and their conviction of a serious crime forfeits certain rights of bodily integrity and privacy relative to the law enforcement system.²¹ With a more comprehensive database, however, especially one in which the entire population is included, neither of these justifications apply. Adding more law-abiding citizens to the database will result in an ever-diminishing percentage of matches relative to the total database. Furthermore, law-abiding citizens have done nothing that could be considered a forfeiture of their right to be outside of the law enforcement system.

The argument has been made that a population-wide database will promote "racial justice" because it will eliminate the current overrepresentation of minority groups in offender DNA databases and the in-

creased overrepresentation of minorities if arrestees are added.²² The overrepresentation of minorities in offender DNA databases reflects the overrepresentation of minorities in the criminal justice and correctional systems, and this overrepresentation is caused by sentencing policies that disparately impact minorities as well as gross disparities in education, employment, housing, health care, and other essential life opportunities. The overrepresentation of minorities among arrestees is caused by "racial profiling" and other dubious law enforcement practices. Having a disproportionate number of minority criminals and suspects is a social problem; it is not a DNA database problem. The solution is *not* a more egalitarian, universal database in which the entire population shares the indignity of inclusion in the DNA database while simultaneously giving greater power to the police.

Sociologist Troy Duster makes a more practical argument in opposition to the claim that a universal database will help eliminate racial bias.

If the lens of the criminal justice system is focused almost entirely on one part of the population for a certain kind of activity (drug-related, street crime), and ignores a parallel kind of crime (fraternity cocaine sales a few miles away), then even if the fraternity members' DNA samples are in the databank, they will not be subject to the same level of matching, or of subsequent allele frequency profiling research to "help explain" their behavior.²³

Thus, it is unrealistic to expect that a "neutral" database policy, layered over an unequal criminal justice system, will eliminate the systemic bias.

Dragnets

In 1987, British authorities collected and tested the DNA samples of approximately 4,000 men in an attempt to find the perpetrator of a brutal, double rape-homicide.²⁴ Although the perpetrator was not one of the thousands of men from whom DNA was collected, he was eventually caught when he attempted to persuade a friend to submit a sample on his behalf.²⁵ The technique of collecting DNA from a large group of individuals to search for the perpetrator of a crime, referred to as a "DNA dragnet," has become a common practice in the United Kingdom, and it is used to a lesser extent throughout Europe and the United States.²⁶ Dragnets often entail the collection of DNA from individuals who fit the general description of a perpetrator, usually residing or working in the same geographic area where the crime occurred,²⁷ and tend to be used in cases in which investigators have not had success obtaining leads using traditional law enforcement mea-

tures.²⁸ It is not unusual for hundreds or thousands of individuals to be asked to “voluntarily” provide a DNA sample.²⁹ The largest known DNA dragnet, conducted in Germany, involved the collection and testing of DNA samples from approximately 16,400 men.³⁰ Whereas some see the DNA dragnet as a valuable, effective law enforcement tool, others describe it as “costly, inefficient and fraught with potential rights violations.”³¹

DNA dragnets have had only limited success in helping to solve crimes in the United States. A 2004 study determined that DNA dragnets had successfully assisted in the capture of a suspect in only one of the eighteen reported dragnets conducted in the United States.³² At the same time, the social costs of DNA dragnets are substantial. Individuals are selected for sampling without probable cause. The sample population frequently consists of members of a single – often minority – racial or ethnic group.³³ Although consent to participate is nominally voluntary, such requests from law enforcement officers are inherently coercive. Many individuals lack knowledge of their right to refuse or the consequences of consent.³⁴ Hesitant individuals are presented with two unpleasant options: “voluntarily” submitting to DNA sampling, or becoming specific targets of the investigation and even being exposed to the public as a suspect.³⁵ In Oklahoma in 2001, people who refused to consent to DNA testing were served with search warrants and treated as suspects, thereby suffering public humiliation.³⁶

Despite the assumptions of many individuals who submit DNA samples, as well as the assurances sometimes given by police, DNA profiles of dragnet volunteers are generally not destroyed after it is determined that the volunteer’s profile does not match the one derived from the crime scene evidence.³⁷ Most state laws do not address the retention or expungement of genetic information obtained from suspects or samples given “voluntarily.”³⁸ Consequently, profiles are often retained in law enforcement databases that are not part of the national system, where they are used routinely to compare against local crime scene evidence.³⁹ There have been multiple publicly reported instances of the police retaining samples after a dragnet was conducted.⁴⁰ In Louisiana, law enforcement officers included in its state offender database the samples of 1,200 men found not to match the biological evidence of a suspect.⁴¹ In Ann Arbor, Michigan, 160 men tested who did not match a rapist’s DNA profile were forced to file a lawsuit to get the police to return or destroy their samples.⁴²

Familial and Personal Searches

Indirect Searches

The genetic similarity of close relatives has permitted law enforcement officials to use the DNA of one family

member to infer whether another family member has been the perpetrator of an unsolved crime. For example, in a rape case in which crime scene DNA does not match any DNA profiles in the CODIS database, the perpetrator may likely be one of ten men who worked in the area where the rape occurred. If these ten men refuse to provide DNA samples voluntarily, and if there is insufficient probable cause to obtain a court order for a sample, the police may attempt to obtain the individuals’ DNA indirectly through family members. Thus, police officers could surreptitiously follow the preschool-age son of one of the men until he discarded some used chewing gum or a tissue. Or, police officers could visit the nursing home where another man’s mother resided and wait for her to discard a paper napkin used at lunch. Then, the item could be seized and analyzed through Y chromosome or mitochondrial DNA markers. In this way, DNA evidence about the potential suspect could be obtained indirectly, without the individual’s knowledge or consent.

Supreme Court decisions have clearly held that individuals have no expectation of privacy in abandoned property,⁴³ and there may even be questions about whether a defendant would have standing to challenge the seizure of a relative’s abandoned property.⁴⁴ Regardless of the constitutionality of the seizure, there is something deeply troubling about police officers performing surveillance of close relatives of potential suspects to obtain DNA samples. It is especially repugnant to think that police surveillance could involve toddlers or senior citizens in nursing homes. Several states have enacted laws requiring consent before a genetic test may be run,⁴⁵ but all of these laws have an exemption for law enforcement. Thus, it may be appropriate to consider statutory or regulatory control of DNA collection through indirect means.

Low Stringency Searches

The forensic testing community in the United States uses a standardized set of thirteen core short tandem repeat (STR) loci. STR markers are sequences of two to six base pair units, and alleles are typically 100-400 base pairs in size. These STR loci typically contain between seven and fifteen alleles (or alternative forms).⁴⁶ Because these markers have such a high degree of polymorphism, on average, unrelated individuals share only about one locus out of thirteen.⁴⁷ Related individuals, however, are likely to share more loci. On average, full siblings share four loci, and there have been rare reports of siblings sharing nine to eleven loci.⁴⁸ In addition, siblings with the same mother will share mitochondrial profiles, and brothers with the same father will have the identical Y-chromosome STR haplotypes.

Knowing that allele sharing of the core loci by individuals likely indicates kinship has important consequences for forensic database searches. Although CODIS rules require correspondence of thirteen loci in order to qualify as a match, it is possible to perform a “low stringency” search in which matches at fewer loci are indicated. Thus, a crime scene sample may have a four or five loci match with a known profile in a database. Such a finding may suggest that a first-degree relative of the person whose profile is in the database may have been the source of the crime scene evidence.

Massachusetts⁴⁹ and New York⁵⁰ are the only two states with regulations explicitly addressing low stringency searches. Both states require that a minimum of four loci be provided for a forensic search against the database, but exceptions are granted. Neither state limits the ability to perform a low stringency search.

At the present time, low stringency searches may not be a particularly valuable use of law enforcement resources. According to Dr. Frederick R. Bieber,

low stringency database searches using the current thirteen-locus STR analysis would be expected to lead to too many partial-profile hits to be of any practical use in the majority of investigations, because many alleles are very common in the population and would be shared by large numbers of individuals.⁵¹

New technologies, however, may increase the utility of low stringency searches.⁵² The Forensic Science Service of the United Kingdom has begun offering “familial searching” to police to aid in investigations. A few well known cases in the U.K. were actually solved using leads developed through low stringency searching.⁵³

Other emerging DNA forensic technologies, such as single nucleotide polymorphisms (SNPs, especially valuable in sorting samples with multiple DNA sources) and low copy number DNA (valuable in typing samples with a minute quantity of DNA), are likely to increase the utility of low stringency searches. These searches would raise the legal and policy issues of whether pursuing suspects because of a low-stringency match with a database sample is somehow an improper use of the database, or otherwise violates public policy.

Surname Searches

Besides obtaining their Y chromosome DNA profile from their fathers, sons usually get their surnames from their fathers as well. It has been suggested that where a rare surname is associated with a distinct Y chromo-

A crime scene sample may have a four or five loci match with a known profile in a database. Such a finding may suggest that a first-degree relative of the person whose profile is in the database may have been the source of the crime scene evidence.

some haplotype, it would be possible to do a surname search after analyzing crime scene DNA.⁵⁴ For this to be possible, a surname haplotype database would need to be established. Then, if DNA analysis of crime scene evidence indicated the distinctive Y chromosome haplotype of, for example, the Darwinsky family, police could check the whereabouts of all of the people in a certain area with the surname of Darwinsky. For a family with a lawbreaking relative, surname searches really could lead to the “rounding up of the usual suspects.” As with low stringency searches, it may be necessary to consider whether special legal or policy measures are needed to regulate law enforcement agencies that have developed the practice of following up on name-based “suspicion.”

Health Care Biobank Searches

If crime scene DNA evidence does not match any known CODIS profiles, and there are known potential suspects, it may be possible to obtain samples of physical specimens from health care facilities for DNA typing. The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA)⁵⁵ contains two provisions specifically dealing with disclosures of individually identifiable health information for law enforcement purposes. First, merely in response to a request by a law enforcement official (conceivably, any police officer) for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, a health care provider may disclose the following information: (1) name and address; (2) date and place of birth; (3) social security number; (4) ABO blood type and rh factor; (5) type of injury; (6) date and time of treatment; (7) date and time of death, if applicable; and (8) a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.⁵⁶ The health care provider may not disclose DNA information, dental records, or typing, samples, or analysis of body fluids or tissue.⁵⁷

More detailed information, including tissue samples, is permitted under a second provision applicable to law enforcement. Health care providers may make disclosures required by law (e.g., gun shot wounds) or disclosures in compliance with one of the following: (1) a court order; (2) a grand jury subpoena; or (3)

an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law.⁵⁸ The request must simply allege that the information sought is relevant for law enforcement purposes.⁵⁹ Of particular significance is the fact that the third method of obtaining information includes a broad class of *ex parte*, non-judicial processes, and showing probable cause is not required.

DNA Forensic Profiling

The previous sections have discussed the collection and analysis of DNA samples from individuals in an attempt to match crime scene evidence. There is another, somewhat different use of DNA-based forensic technologies with important ethical, legal, and social implications. It involves the use of DNA testing of crime scene evidence to develop a DNA forensic profile of the alleged perpetrator.

Law enforcement officials already have the capacity to do some forensic genetic profiling based on biological specimens left at crime scenes. For example, blood left at a crime scene could easily be analyzed to determine whether it came from a male or female, and whether the individual had a distinctive chromosomal or other anomaly such as Down syndrome or Fragile X syndrome. Analyses of other genetic loci could lead to statistical predictions of the individual's race and ethnicity.⁶⁰ It is likely that within a short period of time there will be claims of the ability to make behavioral genetic predictions about such matters as sexual orientation, intelligence, addictive behavior, musical ability, and temperament.⁶¹

Aside from the question of the scientific validity of such associations, are there ethical or legal concerns about genetic profiling to indicate that the alleged perpetrator is, for example, likely to be a tall, gay, white, male, and of Scandinavian ancestry, who is left-handed, has above average intelligence, is shy, with perfect pitch, and is susceptible to addictive behavior? What legal issues are raised by using such profiles to obtain search warrants, to wiretap, or to engage in surveillance? At what stage of the legal proceedings are determinations made of the scientific acceptance of DNA forensic profiling?

Police investigators already use forensic profiling techniques, some of which may be of dubious value. Police routinely use eyewitness recollections of individuals, often reduced to a sketch or computerized composite which sometimes bears little resemblance to the perpetrator. They may also rely on experts to develop a psychological profile of the perpetrator or other measures to narrow or focus an investigation. What, if anything, makes DNA profiling different or wrong?

At least three examples come to mind. First, the use of unproven scientific methods may divert attention from the real perpetrators of the crime to innocent suspects. Second, if behavioral genetic forensic profiling becomes an accepted measure in criminal investigations, it will not be long before prosecutors attempt to use this information at trial as further evidence of the guilt of the suspect. Third, governmental use of any scientific method serves as an imprimatur of the validity of the technique, which could have the effect of increasing the use of behavioral genetic predictions in employment, schools, or other non-law enforcement settings, thereby leading to an increase in the erroneous belief that behavior is unalterably determined or influenced by genes.⁶²

Retention of Samples

With so many samples being collected for the extraction of DNA, critics of expanded databanking are concerned about what becomes of samples after the profile is created.⁶³ There is no national policy on sample retention, but in almost every state the samples are retained indefinitely.⁶⁴ Saving the samples could be useful for retesting or the inclusion of additional genetic markers, but as long as the samples are stored, there is a possibility that they could be used by unauthorized third parties in ways that might lead to disclosure of confidential information, or for malicious, retributive, or oppressive purposes.⁶⁵

About half the states have laws explicitly addressing the retention of DNA samples; the remaining state statutes are either silent or authorize a state agency to establish rules regarding storage and retention.⁶⁶ In some states, expungement procedures explicitly include the actual sample, while others do not.⁶⁷ It is likely, though, that in most states the disposition of the sample would be determined by the policies for expungement after exoneration. Besides expungement, few states provide for the mandatory destruction of samples, allowing us to draw the conclusion that DNA samples are being retained indefinitely in most states, unless (1) the individual has a conviction overturned or case dismissed, or (2) the individual is an arrestee who is never convicted or plea bargains.⁶⁸ Wisconsin is the only state that explicitly requires the destruction of DNA samples after analysis is completed,⁶⁹ but reportedly, no samples have yet been destroyed. Two states to address the retention issue are Nebraska and Arizona. Nebraska requires that all samples be permanently retained,⁷⁰ and Arizona requires that all samples be retained for at least thirty-five years.⁷¹

The process of removing information from an individual's criminal record, which can include a DNA profile or sample, is called expungement.⁷² Not all states

have provisions allowing for the expungement of DNA profiles.⁷³ Thirty-eight states have statutes describing the process of expungement of DNA information, and among those states, the criteria and procedures including what information is expunged, vary by state.⁷⁴ Most states require that the conviction be reversed or the case be dismissed.⁷⁵ However, some states have more stringent requirements. For example, Illinois requires a determination of “actual innocence” (reversal of the conviction or a pardon) before genetic information is expunged.⁷⁶ The majority of states do not provide for automatic expungement upon reversal or dismissal. Instead, thirty-three states require that the offender initiate the procedure for expungement, and only one, Texas, requires that the offender be advised after acquittal of his or her right to expungement.⁷⁷

To initiate the expungement process, most states require the individual to file a request or petition.⁷⁸ The process for expungement in California requires the individual to file a request not only with the trial court, but also with the DNA laboratory and the prosecuting attorney.⁷⁹ Of the states requiring collection of DNA from suspects or arrestees, three (Louisiana, Texas, and Virginia) require that the DNA information be expunged upon acquittal or dismissal of charges.⁸⁰ However, in California, an arrestee’s DNA sample and profile can be retained for up to two years or until the investigating law enforcement agency informs the state DNA laboratory that the person is no longer a suspect in a criminal investigation. The sample can be used in the interim in any database and investigation.⁸¹

In this discussion, “destruction” involves only the samples collected from known individuals. Unquestionably, crime scene evidence should not be destroyed, because it may be necessary to retest it in the future. Unlike the circumstances with crime scene evidence, there is unlikely to be a need to retain the database samples for retesting. If there is some discrepancy, a new sample can be obtained from the individual for comparison with the information in the database from which the questioned match was generated.

Law enforcement officials want to continue retaining database samples indefinitely so that samples can be retested if new technology is developed for identification purposes.⁸² Although possible development of new technology might militate in favor of sample retention, these interests are outweighed by the social cost of retention. Destruction of samples immediately after analysis would go a long way in assuring the public that their DNA will not be used for purposes unrelated to legitimate law enforcement. After the DNA sample is destroyed, the remaining information would consist merely of thirteen sets of numbers with no diagnostic, prognostic, or research significance. The retention of

samples is a leading source of opposition to current DNA database practices, and it will be increasingly controversial if the scope of the databases is expanded.

Other Uses

Although DNA databases were originally established to aid law enforcement, many states now authorize other uses of offender DNA information, including identification of missing persons or unidentified remains, and “other humanitarian purposes.”⁸³ Thirty-four states explicitly authorize the use of genetic information to create a statistical database, and another four authorize the use of the DNA database for statistical purposes.⁸⁴ Of states that authorize the use of their DNA database for statistical purposes, Alabama is unique in that it allows use of its database to “provide data relative to the causation, detection and prevention of disease or disability” and “to assist in educational or medical research.”⁸⁵ There are no federal limits on the use of DNA database information, and only eight states explicitly prohibit the use of the database to obtain information on physical traits, predisposition to disease, or medical or genetic disorders.⁸⁶ Surprisingly, forty states do not address the use of the genetic information in their DNA databases for genetic research.⁸⁷

Balancing Privacy and Law Enforcement

We have noted that the expanded use of DNA in law enforcement raises numerous concerns: (1) increasing the number of individuals from whom a DNA sample may be required on a routine basis; (2) coercing large numbers of individuals to submit samples as part of a DNA dragnet; (3) obtaining DNA samples from close relatives, including children, as a way of indirectly searching the DNA of a suspect; (4) performing low-stringency searches to identify the close relatives of the alleged perpetrators of a crime; (5) accessing biological specimens in health care institutions for DNA testing; (6) using DNA samples for research without the consent of the sample donor; (7) using behavioral genetic forensic profiling based on crime scene DNA; and (8) retaining non-crime scene DNA samples indefinitely.

Each of these uses involves different ethical and legal issues, each has a different significance, and each demands a somewhat different method of analysis. Nevertheless, for simplicity, they may be considered to implicate a similar interest of individuals to be free from having their DNA profile used for law enforcement.

Privacy Interests

The interests of individuals in DNA identification relate to privacy, autonomy, anonymity, secrecy, freedom, and liberty. For ease of discussion, we will call all of these interests privacy. They all deal with the condi-

tions under which law enforcement agencies may require information from or impose other conditions on individuals (e.g., submission of a biological sample) in connection with a criminal investigation or the criminal justice system.

In general, legal limitations on law enforcement activities depend on the nature of the intrusion upon individuals. Because of the varied levels of intrusiveness, law enforcement officers must meet a different legal and evidentiary standard to make an arrest, conduct a nonconsensual search, or obtain confidential information, such as bank records or medical records. What law enforcement standard should apply to individuals' interest in being free from having their DNA analyzed by the police?

To answer this question, we must first consider the issue of genetic exceptionalism, which refers to the treatment of genetic information separately from other forms of health (or in this context, forensic) information. Although legislatures have frequently enacted genetic-specific laws (for reasons beyond the scope of this article), the overwhelming majority of scholars to consider the issue in the context of genetic privacy and genetic nondiscrimination have argued against genetic exceptionalism.⁸⁸ The reasoning is as follows. Scientifically, it is questionable whether health information can be meaningfully divided into genetic and non-genetic information; practically, it is unlikely that health information can be segregated to permit the disclosure of only one type of information; and from a policy standpoint, genetic exceptionalism may make matters worse by reinforcing notions of stigma. These arguments against genetic exceptionalism all have been made in the context of privacy and nondiscrimination. To our knowledge, the issue has not been considered in the context of criminal justice. Do these arguments apply here as well?

Suppose that police are investigating a series of murders at pharmacies in a certain area. All of the murders occurred in the course of an armed robbery in which the robber only took large quantities of an expensive and relatively rarely used prescription drug. Police theorize that the robber is someone who is dependent on the medication. They want to conduct a dragnet in the area to ask people to submit to a blood test or saliva test to check for the presence of the drug. Leaving aside the logic or the likely success of such an investigatory measure, would the public and legal scholars have the same objections to the drug test dragnet as they do to DNA dragnets? It should be noted that the hypothetical drug test will reveal more personal health information about the individual than a DNA test of the thirteen CODIS loci. The DNA profiling is more limited, but more specific. It might provide a match with the crime scene evi-

dence, whereas, in this example, the drug test will only indicate whether the person is among an unknown number of individuals taking a certain medication.

It seems to us that the privacy and civil liberties analysis surrounding expanded use of DNA forensics in law enforcement should not be based on whether the test performed is "genetic." The justification for, the intrusiveness of, and the procedures surrounding a test are at least as important as the type of test performed on a sample. Thus, the legal and policy question should concern the legal basis on which law enforcement personnel require or "encourage" individuals to submit to a biological test of an invasive nature, or infringe upon an individual's dignity. It seems paradoxical that if the police seek to obtain a court order directing a particular individual to submit a DNA sample or to undergo a medical test, the order would not be granted in the absence of probable cause. On the other hand, if police strongly encourage all individuals in a certain area to "voluntarily" submit a sample as part of a dragnet, then a different standard will be applied and the requirement will be generally upheld. Furthermore, some legal scholars have argued that even a statute establishing a universal database would be constitutional.⁸⁹

The prospect of expanded use of DNA forensics needs to be placed in context. In a world in which personal privacy is difficult to maintain against an onslaught of computer file sharing, surveillance cameras, biometric imaging, thermal imaging, and other technological "advances," for many people, the last "off limit" area for access to personal information is law enforcement. Millions of people enthusiastically send their credit card information via computer to unknown merchants and other users. If a police officer asked someone for credit card information however, we doubt there would be the same eager response.

The leading privacy concerns about more inclusive DNA forensic databases are that this powerful information (and the biological samples from which it is obtained) would be collected on a routine basis without any individualized suspicion of wrongdoing, that individuals would be coerced to provide samples in dragnets, that relatives of potential suspects would be tested, and that the original specimens would be retained indefinitely.

Assume that a hypothetical country routinely required all of its residents to submit the following items to the police: a DNA sample, a yearly photograph, handwriting exemplar, voiceprint, fingerprints, hair samples, retinal scans, bank statements, credit card information, health records, and other details of their personal life. Obviously, ready access to this information by police would help solve crimes. Nevertheless, such comprehensive information submission to law

enforcement would be widely viewed as hallmarks of a repressive, totalitarian state, quite different from the United States, with our libertarian tradition and Bill of Rights protecting citizens against unreasonable governmental interference with our lives. We are concerned that the United States not heedlessly proceed in this direction. Fingerprints already are widely available to police and photographs appear on drivers' licenses and passports. Each individual intrusion is easier to defend than the sum of government demands. At what point is the cumulative intrusion by the government unacceptable?

In *Osborn v. United States*,⁹⁰ Justice Douglas warned what can happen when technology is utilized without an assessment of its true value to or effect on society:

[T]he privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen – a society in which government may intrude into the secret regions of man's life at will.⁹¹

Our concern is not that expanded DNA databases would transform our country into a “nation of suspects.”⁹² Our concern is that we would become a nation with unfettered police powers. Moreover, once greater information about individuals is in the possession of police, it will be difficult to prevent other uses of the information by the government.

We recognize the difficulty of deciding when to oppose intrusions by the government undertaken in the name of protecting the public. It is easy to object to outrageous conduct, but, as with DNA forensics, it is harder when there is a seemingly compelling justification for the intrusion on privacy. In the landmark 1886 case of *Boyd v. United States*,⁹³ in which the Court spelled out the scope of Fourth Amendment protections, Justice Bradley wrote: “It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure.”⁹⁴ We believe that in the absence of probable cause or prior conviction, individuals have legitimate interests in not submitting their DNA to law enforcement officials for profiling and retention.

Law Enforcement Interests

The public's interests in law enforcement are more concrete than its privacy interests, and perhaps this is one reason law enforcement interests have tended to prevail in the area of DNA identification. Members of

the public – and not just law enforcement officials – are justifiably concerned about crime. Although we have previously noted our discomfort with the use of “cold hits” and “investigations aided” as the sole measures of the efficacy of DNA databases, we do not question that DNA databases work. DNA databases have helped to solve numerous crimes, including heinous crimes that were unlikely to have been solved without them. To the extent they result in the incarceration of criminals, the DNA databases also prevent crimes by known criminals and serve as a general deterrent. In getting violent criminals off the streets, DNA databases also help ease the psychological burden from crime victims and their families.

We believe that the crime solving and prevention benefits of DNA databases justify the establishment, continuation, and funding of the CODIS system. These benefits, however, do not constitute a blanket justification for the use of DNA in unlimited ways. It is not necessarily the case that if a DNA database containing profiles of rapists and murderers is valuable, then a DNA database with all felons, misdemeanants, juvenile offenders, arrestees, or the entire population will produce significantly more hits and therefore be positive for society. It is also not necessarily the case that if the public supports and benefits from DNA forensics that any expansion, including indirect, low stringency, and dragnet searches, also will have the same level of public support. Each new application and extension of DNA forensics must be independently assessed and weighed against the substantial privacy interests implicated.

Whenever there are any restraints placed on law enforcement, the argument is raised that some criminals will escape detection or go free. Certainly, this has been the argument surrounding the exclusionary rule, where the issue is whether the criminal should go free because “the constable has blundered.” In *Mapp v. Ohio*,⁹⁵ in which the Supreme Court held that the exclusionary rule applies in state criminal cases, Justice Clark responded to this argument by stating: “The criminal goes free, if he must, but it is the law that sets him free. Nothing can destroy a government more quickly than its failure to observe its own laws, or worse, its disregard of the charter of its own existence.”⁹⁶

Law enforcement is essential to the public and an important responsibility of government. Nevertheless, our government was founded on the principle that privacy, dignity, due process, and liberty serve to constrain law enforcement activity. These values are embodied not only in the Fourth Amendment prohibition on unreasonable search and seizure, but also in the Fifth Amendment guarantees of due process, equal protection, and freedom from self-incrimination; in the Sixth Amendment right to counsel; and the Eighth Amend-

ment ban on cruel and unusual punishment. Undoubtedly, there would be more convictions if police could enter homes without warrants and seize contraband and instrumentalities of crime, if they could wiretap and electronically intercept telephone calls without a warrant, if they could coerce confessions, if they could set up roadblocks for any reason at any time, if they were not required to give *Miranda* warnings to suspects, and if they could engage in myriad other practices that are antithetical to our way of life. The golden gift of preventing and solving crime is not worth the price of our liberty.

Conclusion

In writing about the importance of privacy, especially in the context of search and seizure law, the temptation to quote from Justice Brandeis' legendary dissent in *Olmstead v. United States*⁹⁷ is irresistible. In this, the sesquicentennial of his birth, resistance is futile. In *Olmstead*, the majority rejected a Fourth Amendment challenge to wiretapping on the ground that there was no physical invasion. In his dissent, Justice Brandeis captured the essential nature of privacy, and he provided a moving and compelling explanation of why protecting privacy is so fundamental to freedom.

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.⁹⁸

In probably the most frequently quoted passage of his dissent, Justice Brandeis alerted us not to let the exigencies of the day and the beneficent intent of governmental actions weaken our resolve in defending privacy and safeguarding liberty.

Experience should teach us to be most on guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rul-

Our concern is not that expanded DNA databases would transform our country into a “nation of suspects.” Our concern is that we would become a nation with unfettered police powers.

ers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.⁹⁹

DNA databases and their forensic applications must be assigned their proper place in law enforcement. New expansions of DNA technology should not be considered until scientifically rigorous, independent studies demonstrate that the new application would have significant utility to law enforcement. Even then, the expanded use of DNA should be adopted only if it would be consistent with fundamental privacy and civil liberties interests.

Acknowledgements

The authors are indebted to Lori Andrews and Fred Bieber for helpful comments on an earlier draft of this article.

References

1. See T. Simoncelli and B. Steinhardt, “California’s Proposition 69: A Dangerous Precedent for Criminal DNA Databases,” *Journal of Law, Medicine & Ethics* 33 (2005): 279-293, at 282; Reprinted in *Journal of Law, Medicine & Ethics* 34 (2006): 199-213; M. Ballve, “DNA Fingerprinting Trend Threatens Genetic Privacy,” Pacific News Service, July 14, 2004, at <<http://www.alternet.org/rights/19234/>> (last visited February 6, 2006). This article points out that in 2003 alone, over a dozen states changed their laws to expand the scope of their DNA collection.
2. Cal. Pen. Code § 296 (West Supp. 2005); T. Simoncelli and B. Steinhardt, *supra* note 1, at 279.
3. La. Rev. Stat. Ann. §15.609.
4. Tex. Gov’t Code Ann. §411.1471.
5. Va. Code Ann. §19.2-310.2:1.
6. Title X of the Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. Law No. 109-162, 119 Stat. 2960 (2006).
7. See National Institute of Justice, *National Commission on the Future of DNA Evidence*, “The Future of Forensic DNA Testing: Predictions of the Research and Development Working Group,” (2000): at 35 [hereinafter “The Future of DNA Testing”].
8. See A. R. Amar, “A Search for Justice in Our Genes,” *New York Times*, May 7, 2002, available at <http://www.law.yale.edu/outside/html/Public_Affairs/246/yfs_article.htm> (last visited February 6, 2006); D. H. Kaye, et al., “Is a DNA Identification Database in Your Future?” *Criminal Justice* 16 (2001): 4-11.
9. D. H. Kaye, *supra* note 8, at 19.
10. C. Rosen, “Liberty, Privacy, and DNA Databases,” *The New Atlantis* 1 (2003): 37-52.
11. M. J. Boavida, “Portugal Plans a Forensic Genetic Database of its Entire Population,” *Newropeans Magazine*, April 11, 2005, at <http://www.newropeans-magazine.org/index.php?option=com_content&task=view&id=2063&Itemid=121> (last visited February 6, 2006).
12. *Id.*
13. S. Alling, P. S. Lane, Division of Governmental Studies and Services, Washington State University, “National Forensics DNA Study Report,” (2003): Appendix 3d, at 46, available at <[162](http://

</div>
<div data-bbox=)

- www.dna.gov/pubs/gen_interest> (last visited February 15, 2006).
14. These expenses could vary depending on how the samples are collected, analyzed and stored, but would conceivably include the cost of devices and materials for collecting, analyzing, storing, and accessing the data, as well as the cost of training and labor cost of personnel needed to run the system. Although there have been no estimates of the cost of a universal database in the U.S., estimates done in Europe and per person profile costs can serve as a basis for a rough estimate. Based on the conservative estimate of \$60 per person it would cost approximately \$18 billion for the profiles. Based on the £5.5 billion estimate made by the British government for its 60 million inhabitants, it would cost \$50 billion to create a national database in the U.S. (Government estimate of £5.5 billion, others up to £20 billion, for a universal database involving the approximately 60 million people in the U.K.) A. Deane, "Identity Cards in Britain," *Contemporary Review* 286, no. 11672 (2005): 268-270, at 269; M. J. Boavida, *supra* note 11 (estimate of Portugal universal database made at 40-80 euros per person); American Society of Law, Medicine & Ethics, "DNA Fingerprinting and Civil Liberties," *Project Description*, at <http://www.aslme.org/dna_04/description.php> (last visited February 7, 2006), estimating \$50 to \$100 per profile.
 15. CODIS Program, *Mission Statement & Background*, Federal Bureau of Investigation (FBI) website, at <http://www.fbi.gov/hq/lab/codis/program.htm> (last visited February 7, 2006).
 16. According to Dr. Paul Ferrara, Director of the Virginia Division of Forensic Science, more than half the violent crimes solved by the use of the state database involved DNA samples obtained from convicted burglars. R. Willing, "DNA Links Burglars to Harder Crime," *USA Today*, December 7, 1998.
 17. CODIS Program, *Measuring Success*, Federal Bureau of Investigation (FBI) website, at <http://www.fbi.gov/hq/lab/codis/success.htm> (last visited February 7, 2006).
 18. FBI, *Uniform Crime Reports, Crime in the United States*, 1995, 2004, available at <http://www.fbi.gov/ucr/ucr.htm> (last visited February 7, 2006).
 19. R. Willing, "DNA Matches Win Few Convictions in Va.," *USA Today*, November 7, 2005.
 20. See S. McVicker, "More DPS Labs Flawed: DNA Testing Woes Across State Threaten Thousands of Cases," *Houston Chronicle*, March 28, 2004, at A1; K. Herbert, "Crime-lab Mistakes Spark Alert: Hundreds of Pa. Cases May Be Reexamined," *Philadelphia Inquirer*, June 19, 2003, at A01; R. Willing, "Mueller Defends Crime Lab After Questionable DNA Tests," *USA Today*, May 1, 2003, at A03; L. Hart, "DNA Lab's Woes Cast Doubt on 68 Prison Terms: Forensic Science at a Houston Police Unit Was Plagued by Problems. The inmates for Whom Retesting is Ordered Include 17 on Death Row," *Los Angeles Times*, March 31, 2003; R. Stutzman, "State DNA Analyst's Data: Forgeries Could Result in New Trial for Rapist," *Orlando Sentinel*, July 25, 2002; D. Baldwin, "Gilchrist Faces More Scrutiny: Review Ordered in Three Death-row Cases," *Daily Oklahoman*, July 17, 2001; L. Gorman, "The Brady Solution: A Due Process Remedy for those Convicted with Evidence from Faulty Crime Labs," *University of San Francisco Law Review* 39 (2005): 725-727.
 21. *Willis v. Artuz*, 301 F.3d 65, 66 (2d Cir. 2002); *Jones v. Murray*, 962 F.2d 302, 306 (4th Cir. 1992).
 22. See D. H. Kaye and M. E. Smith, "DNA Databases for Law Enforcement: The Coverage Question and the Case for a Population-Wide Database," in D. Lazer, ed., *DNA and the Criminal Justice System: The Technology of Justice* (Cambridge, MA: MIT Press, 2004): 247-284, at 269-271.
 23. T. Duster, "Behavior Genetics and Explanations of the Link Between Crime, Violence, and Race," in E. Parens, A. R. Chapman and N. Press, eds., *Wrestling with Behavioral Genetics: Science, Ethics and Public Conversation* (Baltimore, MD: Johns Hopkins University Press, 2006): 150-175, at 168.
 24. J. Wambaugh, *The Bleeding* (New York, NY: Morrow, 1989).
 25. *Id.*
 26. See J. S. Grand, Note, "The Bleeding of America: Privacy and the DNA Dragnet," *Cardozo Law Review* 23 (2002): 2277-2368, at 2285.
 27. See T. Simoncelli and B. Steinhardt, *supra* note 1, at 285.
 28. F. W. Drobner, "DNA Dragnets: Constitutional Aspects of Mass Identification Testing," *Capital University Law Review* 28 (2000): 479-511, at 485.
 29. T. Simoncelli and B. Steinhardt, *supra* note 1, at 285.
 30. F. W. Drobner, *supra* note 28, at 481.
 31. J. S. Grand, *supra* note 26, at 2280-2281.
 32. K. Bersett, "Victims Challenge Police Use of Controversial 'DNA Dragnets,'" *The New Standard*, at <http://newstandardnews.net/content/?action=show_item&itemid=1044> (last visited February 7, 2006).
 33. American Society of Law, Medicine & Ethics, *supra* note 14.
 34. T. Simoncelli and B. Steinhardt, *supra* note 1, at 285; A. B. Chapin, "Arresting DNA: Privacy Expectations of Free Citizens Versus Post-Convicted Persons and the Unconstitutionality of DNA Dragnets," *Minnesota Law Review* 89 (2005): 1842-1875, at 1859.
 35. S. F. Kreimer, "Truth Machines and Consequences: The Light and Dark Side of Accuracy in Criminal Justice," *New York University Annual Survey of American Law* (2005): 655-674, at n.54.
 36. Editors, "DNA Dragnets," *The New Atlantis* 8 (2005): 104-106.
 37. D. Shepardson, "Suspects No More, They Want Blood Back," *De- troit News*, July 24, 1995, at 1C, noting that police planned to retain for thirty years the voluntarily donated DNA samples of 160 men declared innocent of the crime under investigation; see also M. Hibbert, "DNA Databanks: Law Enforcement's Greatest Surveillance Tool?" *Wake Forest Law Review* 34 (1999): 767-825, at 809, noting that the DNA of convicted individuals who are later exonerated is sometimes not expunged from state databanks; R. Willing, "ACLU Seeks to End DNA Dragnet in Search for Killer in Mass. Town," *USA Today*, January 11, 2005, at 6A, explaining that only one innocent individual has been successful in suing for the return of his DNA sample.
 38. See A. B. Chapin, *supra* note 34, at 1846.
 39. *Id.*; see J. S. Grand, *supra* note 26, at 2283.
 40. J. S. Grand, *supra* note 26, at 2279-2280.
 41. Editors, *supra* note 36; A. B. Chapin, *supra* note 34, at 1842.
 42. K. Bersett, *supra* note 32.
 43. *California v. Greenwood*, 486 U.S. 35, 37, 40 (1988). State constitutional law, however, may recognize an individual's interest in abandoned property. See, e.g., *State v. Goss*, 834 A.2d 316 (N.H. 2003).
 44. *Warth v. Seldin*, 422 U.S. 490, 499 (1975) "[G]enerally [a plaintiff] must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties."
 45. See, e.g., Colo. Rev. Stat. §10-3-1104.7 (2004); Fla. Stat. Ann. §760.40 (West Supp.); Ga. Code Ann., §33-54-3, §33-54-5 (2005).
 46. J. M. Butler, *Forensic Typing: Biology and Technology Behind STR Markers* (San Diego, CA: Academic Press, 2001): 323.
 47. F. R. Bieber, "Science and Technology of Forensic DNA Profiling: Current Use and Future Directions," in D. Lazer, ed., *DNA and the Criminal Justice System* (Cambridge, MA: MIT Press, 2004): 23-62, at 47.
 48. *Id.*
 49. Mass. Regs. Code tit. 515, §2.14 (WESTLAW through November 18, 2005).
 50. N.Y. Comp. Codes, R. & Regs. tit. 9, § 6192.3 (WESTLAW through July 31, 2005).
 51. F. R. Bieber, *supra* note 45, at 48.
 52. F. R. Bieber, et al. (in press).
 53. R. Williams and P. Johnson, "Inclusiveness, Effectiveness, and Intrusiveness: Illusion in the Developing Uses of DNA Profiling in Support of Criminal Investigations," *Journal of Law Medicine & Ethics* 33 (2005): 545-558, at 454. Reprinted in *Journal of Law Medicine & Ethics* 34 (2005): 234-247.
 54. F. R. Bieber, *supra* note 46, at 49-50.
 55. 45 C.F.R. Parts 160, 164 (2004).

56. 45 C.F.R. §164.512(f)(2)(i).
57. 45 C.F.R. §164.512(f)(2)(ii).
58. 45 C.F.R. §164.512 (f)(1)(i),(ii).
59. 45 C.F.R. 165.512 (f)(1)(ii)(C)(1).
60. T. Frudakis, K. Venkateswarlu, M. J. Thomas, et al., "A Classifier for the SNP-based Inference of Ancestry," *Journal of Forensic Sciences* 49 (2004): 1145-1146; F. R. Bieber, *supra* note 46, at 36-37.
61. See M. A. Rothstein, "Applications of Behavioural Genetics: Outpacing the Science?" *Nature Reviews Genetics* 6 (2005): 793-798.
62. *Id.*
63. A. B. Chapin, *supra* note 34, at 1859.
64. S. Axelrad, "Survey of State DNA Database Statutes" (2005) available at <<http://www.aslme.org/dna04/grid/statutegrid.html>> (last visited February 6, 2006). Wisconsin is the only state that requires the destruction of all offender samples after analysis is performed.
65. See *Future of Forensic DNA Testing*, *supra* note 7, at 36.
66. See S. Axelrad, *supra* note 64, at 5.
67. *Id.*, at 4.
68. *Id.*, at 5.
69. Wis. Stat. Ann. § 165.77 (West Supp. 2004) (requiring destruction after analysis has been completed and the applicable court proceedings have ended).
70. Neb. Rev. Stat. § 29-4105 (2005).
71. Ariz. Rev. Stat. § 13-610 (2005).
72. S. Axelrad, *supra* note 64, at 4.
73. *Id.*
74. *Id.*
75. *Id.*
76. 730 Ill. Comp. Stat. Ann. § 5/5-4-3 (West Supp. 2005).
77. S. Axelrad, *supra* note 64, at 4.
78. *Id.*
79. Cal. Pen. Code § 299 (West Supp. 2005).
80. S. Axelrad, *supra* note 64, at grid.
81. Cal. Pen. Code § 297.
82. *The Future of Forensic DNA*, *supra* note 7, at 36.
83. Ala. Code §§36-18-24(e), 36-28-31(b)(3).
84. S. Axelrad, *supra* note 64, at 5.
85. Ala. Code § 36-18-31.
86. See S. Axelrad, *supra* note 64.
87. *Id.*
88. M. A. Rothstein, "Genetic Exceptionalism and Legislative Pragmatism," *Hastings Center Report* 35, no. 4 (2005): 27-33.
89. See D. H. Kaye and M. E. Smith, *supra* note 22.
90. 385 U.S. 323 (1966).
91. *Id.*, at 343.
92. See D. H. Kaye & M. E. Smith, *supra* note 22.
93. 116 U.S. 616 (1886).
94. *Id.*, at 635.
95. 367 U.S. 643 (1961).
96. *Id.*, at 659.
97. 277 U.S. 438 (1928).
98. *Id.*, at 478.
99. *Id.*, at 479.

Copyright of *Journal of Law, Medicine & Ethics* is the property of Blackwell Publishing Limited and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.