In 1987, Tommie Lee Andrews became the first American ever convicted in a case that utilized DNA evidence. On February 21, 1987, a stranger broke into a Florida woman's home in the middle of the night and burglarized and raped the woman at knife-point. DNA samples of semen retrieved from the crime scene matched blood drawn from Andrews, a serial rapist, who is now serving a twenty-two year prison sentence for rape, aggravated burglary and burglary. At that time, no state had a DNA databank. However, after witnessing the power of DNA evidence, state courts and state legislatures would soon grapple with the issue of whether DNA evidence should be admitted at trial as identity evidence and whether establishing state DNA databanks would be feasible and of value to law enforcement. A review of current law reveals that almost every state has embraced and institutionalized the utilization of DNA fingerprinting for crime fighting purposes. For example, just ten years after the Andrews case was decided, all fifty states had laws requiring DNA samples from at least convicted sex offenders. Also, the FBI reports that in the last decade, forensic DNA evidence has been relied upon in over 6800 cases.

Virginia's Story

In 1989, the Virginia Division of Forensic Sciences implemented DNA testing in its criminal investigations, becoming the first state crime lab to introduce such a policy. Later that same year, the Virginia General Assembly became the first American legislature to pass laws that required certain classes of offenders to submit DNA samples for inclusion in a DNA databank. This law required certain sex offenders and certain violent felons to provide samples for the databank. However, just one year later, the legislature expanded the law to require that all felons provide samples for inclusion in the state DNA databank and also required that all felons held in Virginia prisons provide samples upon their release. In 1992, the United States Court of Appeals for the Fourth Circuit upheld the constitutionality of Virginia's databasing system.
The court held that the database was neither a violation of an inmate's constitutional protection against unreasonable searches and seizures, nor did it violate the Constitution's prohibition on ex-post facto laws. Thereafter, in 1996, the Virginia General Assembly further expanded the law to require all juvenile offenders over the age of fourteen to submit samples if they had committed crimes that would constitute a felony had the juvenile been tried as an adult.

Presently, Virginia authorities receive more than 20,000 DNA samples a year, which are added to the more than 150,000 samples that have been collected and stored since 1989. In early 1998, even though only 10,000 of these 160,000 samples had been converted into digitized information, Virginia's Division of Forensic Sciences reported that their state DNA databank had already yielded twenty-six "hits," or connected twenty-six individuals to evidence left at Virginia crime scenes. Furthermore, the Division estimates that the DNA databasing system will assist them in solving at least 600 cases in the next three years.

Forty-nine Other States Established Databanks Within Nine Years

Within nine years of Virginia's establishment of the first state DNA databank, the other forty-nine states passed laws requiring the collection of DNA samples from certain criminals for the purposes of establishing state DNA databanks. All fifty states require DNA samples from convicted sex offenders, with some states collecting from all classes of felons, as well as certain classes of misdemeanants. Additionally, the FBI estimates that most states will eventually begin to collect DNA from all convicted felons when the cost of collecting and analyzing DNA decreases.

Four states require DNA samples from all convicted felons, violent or non-violent, which means, for example, that in New Mexico an individual convicted of felony speeding will have his or her DNA profile included in the state databank. Additionally, at least eight states require the collection of blood from certain classes of convicted misdemeanants, and until 1997 South Dakota's DNA databasing law allowed the collection of samples from persons merely arrested for a crime. Under a Louisiana law effective September 1, 1999, law enforcement officials will collect DNA samples from adults and juveniles arrested for sex offenses or certain violent felonies.

Under Texas law, if an individual was previously convicted of a sex offense, or of burglary with the intent to commit a sex offense, then that individual is required to submit a DNA sample to the state databank upon subsequent conviction for "any offense," which could include non-violent felonies or misdemeanors.

Iowa is the only state that has not statutorily promulgated rules for which convicted felons and misdemeanants shall be included in the state DNA databank, but instead the Iowa law provides that the state's attorney general shall adopt such rules. When making the determination, the Iowa Attorney General shall consider a number of factors, including the "deterrent effect of DNA profiling, the likelihood of repeated violations, and the seriousness of the offense." Additionally, Iowa law allows a sentencing court to determine whether a defendant who will be placed on probation or work release must submit DNA to the state databank. Like the attorney general, the sentencing court must make the determination based on the defendant's personal history and criminal record, "the deterrent effect of DNA profiling, the likelihood of repeated violations by the defendant, and the seriousness of the offense." This provision of the Iowa law also provides that courts shall order DNA profiling "when funds have been
allocated from the general fund of the state, or funds are provided by other public or private sources."

As of January 1, 1999, at least twenty-nine states also required certain classes of juvenile offenders to submit samples for databanking purposes[1] and unlike other juvenile records these DNA profiles do not have to be expunged from the system when the offenders reach the age of majority. Although this may seem to run afoul of our legal system's past practice of allowing juveniles the benefit of beginning their majority with a clean record, at least one court disagreed and found that juveniles are not necessarily entitled to have their DNA profiles expunged from the state database upon reaching majority.

An Arizona appellate court held that the collection, analysis, and databasing of juvenile DNA profiles did not violate the state constitution's provision granting exclusive jurisdiction of juvenile courts to persons under the age of eighteen, nor did it conflict with the state law allowing juvenile courts to destroy juvenile court records once an offender has reached the age of majority.

In 1995, however, an Arizona appellate court held that the state DNA databanking law could not be applied to require the collection of DNA from juvenile sex offenders because the law required collection from "a person convicted of a sexual offense," and juveniles were not "convicted" but adjudicated "delinquent." Subsequently, the state legislature amended the databanking law to include those adjudicated delinquent of sex offenses, and, in 1996, an Arizona appellate court upheld the revised law when two convicted juvenile offenders challenged it. The court held that the Arizona DNA databanking law, which requires juvenile sex offenders to submit a DNA sample for databanking purposes, could not be considered retroactive punishment in violation of federal and state ex post facto clauses. The court stated that the legislature did not intend to "punish" the juvenile sentenced to submit DNA, but enacted the law merely to assist law enforcement officials in solving crimes. Additionally, the court found that laws requiring DNA samples from juvenile sex offenders furthered compelling state interests, such as assisting in investigating future crimes and adult prosecutions of these offenders, and that the laws furthered protective and rehabilitative goals of the juvenile court system by deterring these databanked juveniles from committing future sex crimes.

State Inconsistency in the Face of a National DNA Database

Clearly, state laws are inconsistent in the classes of criminals who are required to donate DNA samples, but these laws also are inconsistent in how their databases can be utilized. Currently, the vast majority of state DNA databanking laws allow their DNA databanks to be automatically searched if done so to assist any criminal investigation or prosecution. However, two state DNA databanking laws authorize their DNA databanks to be searched only if in furtherance of solving sex-related or violent crimes. In North Carolina, the state databank may only be used to assist law enforcement officials investigating "violent crimes against the person." Washington state law allows the DNA databank to be used solely for the investigation and prosecution of sex or violent offenses. Although the limits North Carolina and Washington place on what kinds of investigations may be assisted through a DNA databank search may seem minor, pragmatically these states might unwittingly undermine the effectiveness of their own and other states' DNA databanks when linked into the nationwide DNA database.

For example, DNA databases are not only useful for solving previously
unsolved crimes within one state, but also for solving crimes in other states. Law enforcement officials often contact officials in other states to compare crimes and modus operandi. Similarly, DNA databases can be used to match DNA artifacts left at one unsolved crime scene to DNA artifacts left at other unsolved crime scenes with the hope that a genomic "signature" or fingerprint will prove the crimes were committed by the same person. For example, police in Florida used DNA evidence to determine that four unsolved Florida rapes were all committed by the same person. A search of the Florida DNA database, however, did not provide a link between the perpetrator of the rapes and any previously banked suspect and, therefore, police did not know the identity of the suspect who left DNA at the scene of these four rapes. Eventually, the Florida police asked Virginia and Georgia to search their DNA databases for a profile matching DNA taken from the scene of the four rapes.

One day after their request, Florida law enforcement officials received a call from Virginia's state forensic laboratory which subsequently provided them with the name and social security number of a man whose DNA profile matched the Florida sample. The man, Mark Daigle, had previously been convicted of burglary in Virginia and, consequently, was required to provide a DNA sample for banking. The Virginia conviction and the accompanying DNA sample proved to be the break needed by Florida police. The Daigle case represents the first interstate "hit." The Daigle case suggests that limitations on the accessibility of DNA databanks, such as those in North Carolina and Washington, may foreclose many opportunities to uncover criminal patterns unless the unsolved crime meets the level of seriousness required in order to utilize the other states' databanks.

All states allow their databanks to be used to assist law enforcement officials investigating sex-related crimes. If Daigle had committed non-violent felonies instead of rapes, for example, then Florida officials likely would not have had access to search the North Carolina and Washington DNA databanks to potentially match DNA recovered from their crime scenes. The Daigle case also shows that, in order to maximize the effectiveness of the individual state databanks for these kinds of purposes, there should be a more uniform approach to the utilization of state databanks, at least if the states with these more limited databases wish to participate in the nationwide program. The national DNA database will include only the profiles of convicted felons, and will not include the profiles of misdemeanants or suspects, regardless of whether a state requires collection from these types of individuals. Additionally, the national databank will not limit access based on the type of investigation. Thus, for example, before being linked into the national DNA databasing system, both Washington and North Carolina will be forced to decide whether to allow outside law enforcement agencies full access to their databanks or continue limitations on access based on investigation type. By not allowing others to search their DNA databases except for certain classes of crimes, North Carolina and Washington may be unwittingly undermining the potential of their own DNA databases as well as the efforts of those who are attempting to connect unsolved crimes in their states to those committed in North Carolina and Washington.

At the same time, however, states must not be coerced into expanding the scope of investigations that they believe warrant the utilization of their DNA databases. If the policies of North Carolina and Washington dictate that only the most serious offenders should be subject to the increased privacy intrusion of automatic DNA databank searches, then other states should respect this limitation. Limiting DNA database searches to certain kinds of investigations may mean missing some matches that may have otherwise been made through the database. Yet the limitations North Carolina and Washington have placed on
the accessibility of their DNA databanks are reasonable and effective because they will result in the identification of those criminals with the statistically highest rates of recidivism. However, these limitations will have to be re-examined if these two states wish to participate in the national databank which, so far, only requires that searchers be law enforcement personnel legitimately investigating a criminal offense.

What Is a "Law Enforcement" Purpose?

The fifty state databasing laws currently in force are varied not only in the types of offenders required to submit samples to the DNA databases, but also in the sorts of protections these laws do, or do not, have in place to protect against potential abuses of the information contained in the databases. All of the DNA databasing laws allow law enforcement officials to tap into the database in order to gather identifying information that will be used for "law enforcement" purposes. But what is encompassed within this broad category of "law enforcement" purpose? Arguably, it might include obtaining information about an offender's physical or mental status, such as whether one has a disease like diabetes or schizophrenia, which requires some level of constant medical care. However, using DNA databanking information to gather this kind of information seems to exceed the scope of what constitutes necessary and legitimate information to identify a suspect and link that individual to the scene of a crime.

"Law enforcement" could also include gathering information about the offender's close relatives in certain circumstances. For example, law enforcement officials may have found a DNA artifact at the scene of a crime, but may have been unable to compare this artifact to that of their prime suspect because the suspect has fled and his or her whereabouts are unknown. In this kind of situation, law enforcement officials may argue that it is necessary to compare the DNA of this prime suspect's close biological relatives to that of the DNA artifact from the crime scene to determine whether to continue or cease the pursuit of the suspect...

In 1996, the FBI set up a forensic lab that conducts mitochondrial DNA analysis as an alternative to traditional nucleic DNA analysis; state crime labs are expected to follow suit. Mitochondrial DNA is found outside of the cell nucleus, and a cell contains more mitochondrial DNA than nucleic DNA. Thus, mitochondrial DNA has come into fashion with many forensics laboratories as an alternative to nucleic DNA testing because in many cases it is easier to collect mitochondrial DNA. Pragmatically, this means that a forensics laboratory would be able to extract more mitochondrial DNA from a smaller crime scene artifact, as well as from older or less well-preserved artifacts.

Mitochondrial DNA, however, does not provide the same high degree of unique DNA information that traditional nucleic DNA fingerprinting does because all of a woman's offspring have the same mitochondrial DNA sequence, and the offspring will share that same mitochondrial DNA with all of their maternal relatives for many generations. Thus, it is easy to see how a DNA databank creating digitized profiles either through nucleic DNA fingerprinting or mitochondrial DNA fingerprinting clearly has implications not only for the banked offender, but also for his or her non-banked relatives.

For example, if my sister is convicted of a sex offense, under every state's law she will be compelled to provide a DNA sample, and the identity information gleaned from that sample will be entered into the state databank. Assume that I
have never committed any sort of crime and my DNA is not in the databank. Then assume that a DNA artifact is later found at a crime scene, the genetic fingerprint lifted from the artifact is run through the database, and the conclusion is that although my sister is not a sufficient match, it is likely that one of her siblings is the match. Could this information, obtained in the course of a law enforcement identification, warrant questioning my sister or my arrest as the prime suspect? Ask Robert Flowers' brother.

Robert Flowers was initially the prime suspect of a rape in Indiana. Insisting he did not commit the crime, Indiana police obtained a search warrant and demanded a sample of Robert Flowers' blood in order to compare it to a DNA sample left at the scene of the crime. Indeed, his DNA did not sufficiently match that recovered from the crime scene. However, Robert Flowers' DNA was so similar to that of the sample retrieved at the crime scene that the laboratory suggested to police that the DNA might belong to a relative of Robert Flowers. Eventually Flowers' brother, Danny Flowers, was arrested and convicted of the rape.

This example may not seem terribly insidious. It may have, after all, gotten a rapist off the street. But the fact remains that the justification given for databasing certain classes of criminals' DNA is that it is a necessary crime fighting tool that can be used to deter, condemn, or exculpate individual offenders whose statistically high recidivism rates suggest they may offend again. The argument is that the state is free to reasonably intrude on their privacy interests by digitizing and releasing their genetic fingerprints because they have proven themselves to be offenders. However, this justification cannot be applied to the individual's previously non-databased sibling or other biological relative. They have not committed a crime that warrants this level of privacy intrusion, even if it can be viewed as falling under the rubric of "law enforcement" and, therefore, is permitted by state statutory law.

Considering the inmates' questionable claim of privacy to protect their identification and the minimal intrusion resulting from taking a small sample of blood, the Commonwealth's interest in combatting and deterring felony recidivism justifies the involuntary taking of the sample and the creation of the DNA data bank as reasonable in the context of the Fourth Amendment.

Our legal system recognizes that people have a right to control confidential information about themselves in a number of contexts, such as medical and financial records, and a state may only infringe on this right for a legitimate reason. However, courts in Virginia and other states have held that the state's legitimate interest in the identification of a criminal suspect justifies a "cold" search of databanked offenders without first showing probable cause. Of note, however, at least one dissenting judge in Virginia argued that it is dangerous to assume that a search of one's genome is not unlike the search of one's prison cell, and that "an individual has a reasonable expectation of privacy within one's own body [which] applies equally to prisoners, unless the prisoner's privacy right is incompatible with the objectives of incarceration." Even assuming that it is ethically and legally legitimate to bank and routinely search the genome of past criminal offenders, the same argument could not reasonably be applied to an offender's previously non-banked sibling.

When a suspect is arrested upon probable cause, his identification becomes a matter of legitimate state interest and he can hardly claim privacy in it. We accept this proposition because the identification of suspects is relevant not only to solving the crime for which the suspect is arrested, but also for maintaining a permanent record to solve other past and future crimes .... As with [traditional]
fingerprinting, therefore, we find that the Fourth Amendment does not require an additional finding of individualized suspicion before blood can be taken from incarcerated felons for the purpose of identifying them.

Our criminal justice system is premised on the notion that one can only be penalized after one commits an offense; one cannot be punished merely for having the propensity to offend. Similarly, the Constitution could not permit a sibling to be criminally punished merely for the status of being related to an offender, nor could it be said that a sibling loses privacy expectations of being free of searches merely because he is related to an offender. But were a law enforcement official to use a DNA databank as a tool to gather information not about an offender contained therein, but about an offender's sibling, that official would be conducting a genomic search on an assumed innocent person without having to first justify this level of intrusion - without having to show probable cause for the genomic search.

Gathering information about a databanked criminal's sibling runs afoul of the justification that databanked criminals, by virtue of being criminals, have surrendered a degree of privacy and, therefore, it is acceptable to have their genome digitized for all law enforcement officers to share. The Supreme Court has repeatedly held that criminals cannot expect the same measure of privacy as a non-offending citizen while they are under government incarceration or probation. But where a law enforcement agency, either purposefully or incidentally, gathers information about a non-banked individual by comparing a DNA artifact to his or her sibling's profile digitized in the system, the state is intruding on the privacy of an individual who likely has not committed any act warranting this level of genomic intrusion.

Despite these ethical and constitutional concerns, incidental familial surveillance is encouraged in some states. Most state DNA databanking laws allow the systems to be searched to assist law enforcement agencies in the identification of missing persons. Kentucky, Montana, and Wyoming even go a step further and statutorily allow "close biological relatives" of missing persons to have their DNA profile included in the state DNA database system because having the similarity of their genetic profiles on file will assist in the identification of an unidentified living or dead body. This suggests that familial linkage is already commonly recognized as being within the power of DNA databanks.

By voluntarily including themselves in state DNA databanks, the close biological relatives have chosen to allow the government and law enforcement officials to invade their privacy. Despite the argument that the identification of missing persons is a compelling state interest, state legislatures have not enacted laws requiring the biological relatives of missing persons to provide DNA samples. n85 At the same time, however, these legislatures have not explicitly prohibited the use of the state DNA databanks to gather information about one's siblings, and, therefore, have not foreclosed the possibility that DNA banks will be used in this manner.

Expungement of DNA Profiles of Those Later Deemed Wrongly Convicted

In November 1997, two men were released from prison after DNA evidence proved that they did not commit the crime. In 1986, Donald Reynolds and Billy Wardell were convicted in Illinois of raping a student and subsequently spent eleven years behind bars, continuously stating that they were innocent. In July 1997, a DNA artifact recovered from the crime scene was analyzed in a Maryland lab, and it proved that the semen was neither Reynold's nor Wardell's.
The police now intend to run the semen collected from the rape through the state's DNA databank to see if they can match it to a previously convicted sex offender.

Unfortunately, however, it may be that both Reynolds and Wardell will be considered sex offenders for the rest of their lives, at least according to the DNA databank. Illinois law requires all convicted sex offenders to submit a blood sample if they are sentenced to incarceration or other institutionalized care and to provide such sample as a condition of parole or release, or if they are on parole in another state but are seeking residency in Illinois. Furthermore, the law states that "all information obtained under this Section [which requires the collection of DNA profiles from sex offenders] shall be maintained in a single data base and may not be subject to expungement." A literal reading of the Illinois law would mean that someone who has, as a convicted sex offender, submitted his or her DNA samples to the state DNA databank is not able to have the resulting DNA profile expunged from the databank even if he is later cleared of the crime. Therefore, if Reynolds and Wardell had submitted a sample to the state police while they were incarcerated, even though they have been since cleared of the crime, their profiles do not necessarily have to be purged from the system.

Illinois may not be the only state where an innocent person's DNA could remain in the DNA databanking system. Many states' DNA databanking laws do not explicitly require expungement at all. At least eleven states do not have specific statutory expungement provisions and, therefore, it is unclear whether a wrongfully convicted person could be "exonerated" from the DNA databank. For example, Michigan law requires the permanent retention of all profiles in the state databank gathered post-conviction. However, the law does not require the expungement of these samples if the conviction is subsequently overturned.

Despite the few states like Illinois, many states require both the expungement of the DNA profile from the system and the destruction of the DNA samples once a person has been found to have been wrongfully convicted of the crime for which the sample was collected. Some of these laws have been poorly worded though, which may lead to problems in the future. For example, Maryland requires that the DNA sample and profile be expunged from the system once the conviction leading to the collection of the sample is overturned. However, the statute states that only identifiable information contained in the "statewide DNA data base system and the statewide DNA repository" is subject to expungement, therefore leaving open the possibility that information which is in a national databank may not be expunged. The laws of Maine, Massachusetts, Montana, and Wyoming provide that only the DNA record must be expunged upon finding that a person has been wrongfully convicted, but these laws do not require the destruction of the DNA samples themselves.

Expunging DNA Profiles Gathered from Crime Scene Where It Is Later Shown the DNA Profile Belongs to a Non-Suspect

One of the major purposes of a DNA databank is to serve as a catalog of DNA profiles from evidence or artifacts left at crime scenes. These DNA profiles are entered into the system with the hope that the profile from the artifact, which may belong to the perpetrator of the crime, will match a profile already contained in the system. But not all DNA evidence found at a crime scene will belong to the perpetrator of the crime, especially if the crime scene is not an extremely isolated area. People leave a DNA trail almost everywhere they go; "a hair, saliva on the end of a cigarette butt, perspiration in a hat band, [or] the
most minute amount of blood or seminal fluid" can all provide a DNA fingerprint. But DNA profiles lifted from these types of artifacts found at a crime scene can become valuable leads to suspects if law enforcement officers are able to compare and match these profiles to those of DNA-databased convicted offenders. But finding a match between the artifacts and a known offender should not end the inquiry; further evidence will be needed to connect the suspect to the crime, rather than merely connecting the suspect to the crime scene. For example, the crime scene may be a highly traveled area and a DNA fingerprint lifted from a crime scene may belong not to the perpetrator of the crime, but to someone who had innocently been in the area before or after the commission of the crime. Michigan, a state that does not require the expungement of samples of individuals whose convictions are later overturned, also authorizes this kind of artifact profile to be retained "only as long as it is needed for a criminal investigation or criminal prosecution broad language of this provision may raise concerns over how long the profile may be retained or if the crime scene artifact may be retained. For example, law enforcement officials may decide initially that the DNA artifact belongs to a non-suspect, but might decide to keep the sample in the databank indefinitely until another person is suspected and/or convicted of the crime. But some crimes go unsolved for years and may never be solved and this provision, therefore, would seem to allow the retention of that DNA artifact profile in the system almost indefinitely.

Alternatively, New Jersey law would likely have the exact opposite effect.

New Jersey's provision governing expungement of DNA profiles from its system states, "If one of the bases for inclusion in the DNA database was other than conviction or adjudication, that entry shall not be subject to expungement." This creates an anomalous situation - New Jersey allows the expungement of the DNA profile from a wrongly convicted person, but does not allow the expungement of a DNA profile from the system if that person was included for reasons other than conviction. Nor would New Jersey law require the expungement of a DNA profile lifted from the scene of a crime, even if the suspect who "owns" that profile is later deemed not a suspect. This expungement prohibition raises a legal problem because once New Jersey becomes part of CODIS, the national DNA databanking system, an innocent person's profile will be available for comparison just as would a known offender's profile. The state does not have a rational basis for including the innocent person's profile in the DNA databank, however, because the innocent person has not shown a propensity to offend, nor has the individual done anything to warrant this kind of privacy intrusion. . .

States should also be required to expunge from the system any samples erroneously obtained once a suspect is cleared or a conviction is overturned. In the face of a nationalized DNA databank exchange, even those states that have expungement provisions may fail to expunge all erroneous or incorrect information from the system. Currently, only New Mexico has created an affirmative, statutory duty to ensure that those samples and profiles erroneously contained in the state DNA databank are expunged not only from the state DNA databank, but also from CODIS. Those states that intend to participate in the national DNA databank exchange must also enact this kind of provision to ensure that all such profiles and samples are removed from all criminal DNA databases.

**Conclusion**

Societal pressure to solve crime creates incentives to push forensic DNA
technology as far, and as fast, as possible. Concurrently, DNA technology is rapidly progressing. And yet, state laws currently fail to address the myriad novel social, individual, and legal issues DNA technology presents. Thus, to maintain the legitimacy of DNA databanks, state legislatures must update and refocus DNA databanking laws to provide stricter quality control mechanisms and privacy protection.

[1]