State and National DNA Databases in the Criminal Justice System: Benefits and Obstacles

Andrea Pynaker

Senior Honors Thesis
Submitted in partial fulfillment of requirements of the College Scholar's Program
North Central College

June 2000

Approved Date: 6/6/00

Dr. Louis Corsino, Thesis Director

Date: 6/6/00

Prof. Judy Walters, Second Reader
TABLE OF CONTENTS

Introduction ............................................................................................... 1

Ballistics ............................................................................................. 1
Fingerprinting .................................................................................... 2
DNA Printing ....................................................................................... 4

State DNA Databases ............................................................................. 7

National DNA Database ........................................................................ 13

Challenges and Concerns of a Democratic Public Regarding a National DNA Database ........................................................................ 18

Conclusion .......................................................................................... 25

Bibliography ....................................................................................... 27
THESIS ABSTRACT

The criminal justice system has undergone many changes due to advances in technology. This particular thesis is concerned with DNA databases and the impact they have made on law enforcement agencies and the society that these agencies police. There are numerous technological challenges that have been overcome, and still many that stand in the way in regards to these databases of DNA samples. In addition to the technological difficulties, there are considerable social and political issues that stem from the idea of a national database of DNA information. This paper will include a brief history of databases in the field of criminal justice, a description of the databases on the state and national levels, and an overview of the concerns a democratic society encounters when confronted with the idea of an overwhelming police force with access to highly personal information.
INTRODUCTION

Over the years, the police and law enforcement agencies in the United States have been in search of new and better ways of apprehending criminals through technological advances. Two of the first technological innovations used by police were ballistics and fingerprinting techniques. These enabled the police to better determine which types of weapons were used in criminal incidents and who was at the scene of the crime. With the advent of modern computer technology, we are seeing this information about weapons, ammunition, and fingerprints found at crime scenes stored in databases rather than in paper files as in the past. Access to these banks of information is available to law enforcement agencies, and this has been an additional tool in catching the perpetrators of crimes. Since 1967 the National Crime Information Center has kept a national index of "theft reports, arrest warrants, stolen property, and missing persons that officers in the field can access within seconds" (Byrd 2000). This index is one of the most used federal crime databases, having approximately 2 million inquiries and transactions conducted each day by local and state authorities. We are now at a point in time when a new way of capturing criminals will take center stage – specifically, DNA databases. Before we examine this new technological innovation, however, a brief look at the history of the two previous ways of discovering possible criminals from evidence left at a crime scene may be useful.

BALLISTICS

Ballistics began to be accepted as a legitimate form of evidence in trials around the early part of the 20th century, though the first limited use of this as a type of detection came much earlier, in the 1800s. Widespread recognition of ballistics in the courts, as a
legitimate means of identification, was primarily the result of several key criminal investigations. One event in particular brought the public in closer contact with the advances that had been made in this area — the St. Valentine’s Day Massacre in 1929. Al Capone’s mob slaughtered seven men and police involvement was suspected. In the end, ballistics experts were able to determine that the guns held by the police were not involved with the crime because it was determined that the victims were killed by submachine guns and 12-gauge shotguns, and the police did not carry these kinds of weapons. Later events in the 1960s — in particular, the assassinations of President John F. Kennedy, Senator Robert Kennedy and Dr. Martin Luther King, Jr. — also captured the attention of the public as to what this type of identification could do in apprehending criminals. After these incidents, many commissions and committees were formed and ballistics experts were called upon to provide valuable information. This led to the development of many local ballistic databases. A move to compile this information was called for and the FBI answered this by creating the National Integrated Ballistic Information Network (NIBIN) which contains a database on links between cartridges and weapons used in crimes. Currently there are upwards of 185,000 images entered into the system and these provide police with investigative leads that otherwise might have gone unnoticed. (Hamby 1999)

FINGERPRINTING

Another progression in compiled data was the information gathered from a print of one’s fingertip. This method of detection has a long history. For example:

Pre-historic picture writing of a hand with ridge patterns was discovered in Nova Scotia. In ancient Babylon, fingerprints were used on clay tablets for business
transactions. In ancient China, thumbprints were found on clay seals. In 14th century Persia, various official government papers had fingerprints (impressions), and one government official, a doctor, observed that no two fingerprints were exactly alike. (AIMES)

As the quote above illustrates, this is not a new invention. It was just a new way of using the ancient identification method. The first published account of the reemergence of fingerprint usage was in a letter scripted in 1880 in Britain. It chronicled the fact that a man from India had been using fingerprints as a means of identification since 1858. The first criminal conviction based on fingerprint evidence took place in 1911. In 1924, an act of Congress established the Identification Division of the FBI. By 1946, the FBI had processed 100 million fingerprint cards in manually maintained files and by 1971 200 million cards.

With the introduction of Integrated Automated Fingerprint Identification System (IAFIS) technology, the files were split into computerized criminal files and manually maintained civil files. Though many of the manual files were duplicates, the records represented somewhere in the neighborhood of 25 to 30 million criminals and an unknown number of individuals in the civil files. Currently a new system, costing $640 million, holds the fingerprints of 35 million people (Responsive Database Services 1999). New fingerprint sets from criminals, numbering around 5000, are added daily and 40,000 cards are processed each day. This new collection of data allows the FBI to respond quickly to requests for fingerprint checks, providing “two hour turnaround for requests from local police and a 24-hour time for civil requests” (“Law Enforcement Eases Access…” 1999). The process had previously taken eight days.

The system works by extracting minute details and feature vectors that are used to develop a fingerprint pattern. Using these data and an algorithmic formula, the pattern is
compared to a subset of prints on file that bare a close resemblance to the found pattern.

This eliminates many of the paper problems and human decisions that had been a problem in the past, and replaces them with advanced computer pattern recognition.

With this new system, fingerprints are taken at a local police station and electronically scanned into a computer that sends this information to the database maintained by the FBI. The print is also housed in each state’s individual database. This technology is expensive but it has proven its worth by the vast number of leads it has given law enforcement agencies across the country. By the end of 2000 nearly half the states in the United States will be connected to the IAFIS. However, the most recent technological advance in law enforcement, DNA printing, is more complex than previously utilized techniques. We turn now to an explanation of this most recent printing procedure. ("Law Enforcement Eases... 1999)

DNA PRINTING

DNA printing is a relatively new technique that is still changing and growing. Currently there are various ways in which the testing is done. The simplest form of DNA printing involves the process of cross matching two strands of DNA. In practice it has become one of the most powerful and widely known applications of biotechnology today. There are various techniques to identify the matches. All organisms are made up of living cells that contain DNA, the collection of chemicals represented by the letters A, C, G, and T. These chemicals link to form genes that spell out the specific directions for making up each organism. Every living thing (with the exception of identical twins or those who have received bone marrow transplants) has a unique combination of genes. Certain enzymes, when mixed with a sample of genetic material (body tissues such as
skin or hair, bodily fluids such as blood or semen) recognize specific combinations of the letters A, C, G, and T and "cut" the DNA whenever they encounter that combination. A number of these cuts are made and their positions recorded. The "cut" genetic sequence fragments compose a DNA pattern, or "fingerprint," unique to each person. Finding a match in the genetic sequences from two different "cut" samples provides very strong evidence that both samples came from a single source or individual.

Polymerase chain reaction (PCR), another technique used in DNA comparison, is a faster and more accurate form of detection. PCR essentially mimics the process by which single cells duplicate DNA when they replicate into two cells. Using this process (and by accelerating the process) a large amount of DNA can be created in a matter of hours. Analyzing these large samples makes it much easier to identify matching genetic sequences. Conventional DNA typing can take around 60 days and is very costly when conducted by a private lab. PCR typing can be done in a matter of days at a fraction of the cost. The use of this typing has been in place in the United States since the early 1980s.

Beyond these technological advances, the most important stage in making DNA an essential aspect of modern criminal justice methods was the Violent Crime Control and Law Enforcement Act of 1994 along with the DNA Identification Act of 1994. This act provided funding to state and local crime labs to initiate, upgrade, or expand DNA testing for casework and for DNA database implementation. This worked in conjunction with the FBI's Combined DNA Index System (CODIS) to assure compatibility among local, state and federal databases.
With these technologies and laws now in place, the use of DNA printing has become a very important part of the criminal justice system. Accordingly, the focus of this paper will be on the sampling and comparison of DNA, the current systems used to house the data extracted from these samplings, and reactions to this new way of criminal detection. In particular, this paper will explore databases currently in use in the United States at the state and national levels, focusing on describing the differences between the systems and how they are used. In addition, this paper will examine the concerns regarding the more widespread use of DNA testing and look at possible regulations that must be considered in the future to protect those in danger from the misuse of this technology while still allowing it to suit the justice system.
STATE DNA DATABASES

DNA and the uses for it are all around us. An article in The National Journal (February 2000) states there are currently 5000 separate law enforcement agencies around the country that have their own systems and databases for cataloging criminals: these include states, cities, counties and townships. Since the early 1990s every state has been taking DNA from convicts for use in crime detection and storing the information in local and federal databases. The first state to house one of these banks was Virginia, and it currently houses the largest state bank in the nation. Florida, Illinois, and New York are also leaders in this DNA law enforcement tool. Currently the trend is moving towards the collection of more DNA samples from suspects – not only those who commit violent or sexual crimes but even those who are merely picked up for questioning for a crime.

There are many examples of why these methods are currently in place and how they have led to the convictions of repeat offenders and the exonerations of wrongly accused individuals. (Callahan 2000; Derienzo and Moosy 1999). On November 25, 1991 a masked man entered the home of a couple in Illinois. He shot and killed the husband, raped and shot the woman, and left her for dead. The wife survived the events, but because she was unable to identify the attacker, the police had little to go on. The authorities performed a routine DNA test from a sample of the murderer’s semen and stored the results in their computerized DNA index system. The following April, police in Springfield, IL took a DNA sample from a man convicted of raping a girl and entered the data into the same computer. A match was made and a jury convicted Arthur Dale Hickey and sentenced him to death. (Garfinkel 1997)
Hickey’s case demonstrates the power of DNA indexing systems even at a state level where there are few entries in the database. “DNA is often left at the scene of a crime — a drop of blood, a smear of semen, or a few pieces of hair ripped from the roots” (Garfinkel 1997). This DNA can be analyzed and stored in a computer until it is needed, if ever. Studies show that matches are likely. According to the FBI, 67 percent of rapists commit more than one offense. These databases were created to bring such repeaters to justice in a more efficient manner. Today, the odds of a mistake occurring while matching DNA is around 1 in 100 million. (Garfinkel 1997)

Hickey’s story takes place in Illinois, but there are quite a few of these stories. In the past decade, according to the FBI, some 400 DNA matches have assisted in 600 investigations. Every state since the early 1990s has been taking DNA from convicts for use in crime detection and storing the information in local and federal databases (in some cases, both). In Indiana, a law was passed in 1996 calling for the testing of each inmate that entered the Indiana penal system. In early January 2000 the state’s work on this collection of data paid off when three matches were made in unsolved cases. The state’s collection houses 20,000 convicts whereas prior to the 1996 law state police had told local law enforcement not to send them biological data because they had no basis for comparison. Now Indiana State Police Superintendent Melvin Carroway is urging local law enforcement organizations to send his agency DNA samples from the 500 or so violent crimes that go unsolved statewide each year. “This is a crime-fighting tool of such proportions that I envision it as the same as fingerprinting in the beginning of law enforcement,” (Callahan 2000).
This particular Indiana database, spoken of by Melvin Carroway, was approved by Indiana's General Assembly in 1996 allowing "blood samples to be taken from every inmate convicted of a crime against persons - homicide, sexual assault, batteries, and burglaries." The Department of Correction began taking these samples of incoming inmates in November of that year. Ten thousand additional inmates who were in prison as of July 1, 1996 were also sampled. These samples remain in the database after a convict is released and 3,500 new convicts are added annually. Of the 20,000 convicts in the collection, around 3,000 are released each year after serving their sentences. The compilation of all this information is not inexpensive - federal grants totaling $1 million have been spent on the DNA typing program and the state has contributed $100,000. Major Robert Conley, director of Indiana's four state labs, believes it is all for good reason: "It's sort of an incentive for them (criminals) after they are released to not commit a crime. But if not, it's a way for us to catch up with them." (Callahan 2000)

The states differ in their laws governing the steps of the process -- who is sampled, if and for how long these samples are kept, and who has access to records. Virginia was the first state in this country to open a DNA databank 11 years ago. They currently store upwards of 190,000 samples and as of late 1999 had identified 55 suspects from DNA matches. At the same point in time, Florida, with a base containing 58,000 samples, had identified 180 suspects. According to statistics in both states, in approximately 55 percent of those cases the suspect had a prior conviction for a property crime (Hansen 1999), corroborating FBI's findings on repeat offenders. Somewhat in response to this, several states are moving to expand the number of crimes for which convicted felons will be subjected to having their DNA sampled for the database. Most
states currently take DNA only from those convicted of certain violent or sexual crimes. Florida, for example, has this policy. Massachusetts' Supreme Judicial Court approved a state policy to take DNA from people convicted of 33 different offences in April 1999. Virginia is one of the few that collects samples from every convicted felon passing through their system. The police commissioner of New York City recommended that DNA should be taken from anyone who is arrested and fingerprinted. There are many differing opinions and laws from state to state, but the evidence is there showing the many successes gleaned from the small, individual collections each state has. (Hansen 1999)

Integrating these databases is still a daunting task, however, even though experience suggests that connecting all the information would solve additional crimes. In June of 1999, agents of the border control in Texas picked up a drifter from Mexico. They conducted a search of their state's database to see if this drifter had any outstanding warrants, and finding none, they sent him back to Mexico. Two days after these events a woman in Texas was found beaten to death in her home and a day after that a Houston woman was also found beaten to death. The drifter, Rafael Resendez-Ramirez, is suspected in both of these murders because of the similarities between them. What the Border Patrol did not know was that the FBI was searching for him and that the Houston police had already informed the Immigration and Naturalization Service that he was wanted for questioning. Because of the lack of communication between these law enforcement agencies, Resendez-Ramirez slipped through the hands of the officials. Most certainly the Border Patrol would have kept Resendez-Ramirez in custody if they had known the FBI and Houston authorities were looking for him.
Another piece of this story only supports the frustrations felt by survivors of those murdered by a serial killer: the story of Christopher Maier and his girlfriend. These two young people were the first to be victimized by Resendez-Ramirez. Christopher and his girlfriend, students at the University of Kentucky, were attacked late at night while taking a shortcut by railroad tracks on their way to a party. Maier was beaten to death and the girlfriend was raped, beaten, and left for dead. Thomas Maier, father of Christopher, wonders if a national index of DNA samples could have lessened the 21 months it took to solve the murder of his son. This murder took place in Kentucky and even though the FBI’s index had gone into circulation nine months before that state was not yet a participant. “As a result,” Thomas Maier said, “DNA samples collected from the scene of his son’s August 1997 slaying in Lexington proved largely useless in the search for the killer” (Whitmire 1999). The additional significance of this statement is that Resendez-Ramirez is thought to have gone on to kill seven other people (the Texan women included). (Byrd 2000; Whitmire 1999)

Another case occurred in 1993 in Granbury, Texas where a very frustrated group of police officials were looking for the assailant of two young girls, aged 10 and 11 who had been sexually molested. The girls could not identify their attacker, but he left them with a significant clue: a sample of semen on the girls’ clothing. The crime went unsolved -- the sample of semen did not match any of the samples in the banks in Texas because of the small amount of information housed in them at that time. Two years later, in a nearby Texas town, Lester Parks was convicted on a charge of sexual assault. “Pursuant to Texas law, authorities drew blood from Parks, obtained a sample of his DNA and eventually ran it through a state database” (Higgins 1999). Park’s DNA was a
match to the semen in the Granbury molestation case. Confronted with this information, Parks confessed, and he is currently serving a life sentence. (Higgins 1999)

The stories of these states’ successes should provide some indication how important the advent of DNA technology is to law enforcement. The examples cited above point to crimes that might have been eliminated or solved more quickly, at the state level, if DNA databases had been in place. The specific cases listed above detail the states’ criminals taken out of circulation by this evidence, and the story of Resendez-Ramirez shows the dangers of a state not employing the technology at its disposal. Now the paper will move to examining the database Christopher Maier and his girlfriend could have benefited from – a national collection of criminal DNA samples.
NATIONAL DNA DATABASE

As the information above indicates, database utilization leads to more criminal arrests. The number of these arrests would likely increase if the scope of the database was at a national level. For the past 10 years, DNA technology has been one of the most, if not the most, revolutionary changes in law enforcement. According to FBI spokesman Paul Bresson, “Now with the national DNA database system, it really helps DNA technology to reach its full potential.” The FBI has played a major role in this DNA advancement and currently houses many national databases of criminal information that are available to a variety of law enforcement agencies across the country. In the past 10 years the amount of information available to law enforcement agencies has grown substantially.

The ballistics database (NIBIN), detailed in the Introduction of this thesis, came into being only in 1995 and four years later the fingerprint database (IAFIS) was up and running. CODIS, the national DNA database, was introduced in a trial run in 1995 and is coming close to having all 50 states hooked up and able to go online. It is a national database of DNA profiles from convicted offenders, unsolved crime scenes, and missing persons. The FBI provides access to CODIS free of charge to public forensic labs that perform DNA examinations. Currently it has recorded over two hundred matches linking serial rape cases to each other or identifying suspects by matching crime scene evidence to known convicted offenders. Laws for sampling particular criminals and storing the information in DNA databases have been passed in 49 states, and the last state without such a law, is expected to pass a similar one some time in early 2000. (Niezgoda Jr. and Brown 1995)
CODIS organizes DNA data with two indexes. The Convicted Offender Index contains DNA profiles of those charged with felony sex offenses and other violent crimes. The Forensic Index contains DNA profiles from crime scene evidence (hair, blood, semen) where victims or suspects had not been identified as of yet. These two databases are used to see if any of the samples between them match. This cross-referencing technique opens up leads in cases where the bulk of the evidence is DNA-based and law enforcement has little else to go on. This approach reveals an additional avenue for them to look into; an avenue previously closed to them because the technology was not available. (Mayer 1998)

The system specifications (as of late 1998) has the CODIS records stored on a Microsoft Server database that resides on a pair of 200-MHz Compaq ProLiant 6500 servers that each houses 1 gig of RAM and a 20 gig hard drive. These servers dwell in a secret location. Windows NT is the operating system of choice, and PCs using as low a system as Windows 95 can access it. The application was developed by the FBI with the help of a private corporation and uses Visual Basic and C++. “Ten years ago, forensic examiners were passive individuals, waiting for investigators to bring them leads,” said Dwight Adams, chief of the FBI’s Scientific Analysis Section. Currently, forensic examiners can run searches against the database for matching DNA profiles. When a match to a sample in the Forensic Index is made, crime scenes can be linked and investigators can determine if crimes are related – this allows for a more active role for forensic experts. (Mayer 1998)
The National DNA Index System (NDIS), the final component of CODIS, was launched in 1998. It is a repository for DNA profiles submitted by participating states. NDIS gives state and local police access to the FBI’s database and, more importantly, to the DNA collected by labs in other jurisdictions. This allows for interstate searches and an easy exchange of DNA profiles. In the first half of 1998, two hundred matches were made using the NDIS system – and that was just the pilot run. This was an expensive venture and Congress appropriated $5.5 million between 1996 and 2000 for CODIS’ development. (Mayer 1998)

Of late, a proposal that calls for a compilation of databases with inter-accessibility is on the horizon. Says Paul Kendall, the general council for the Office of Justice Programs. “... we’re trying to facilitate the development of the capability that would allow all the myriad databases around the United States to share information.” The actual stated goal would be to allow law enforcement at all levels to use a Web crawler of sorts to search databases housed in all other jurisdictions. These jurisdictions could, conceivably, exchange files, data, fingerprints, arrest records, and outstanding warrants; this may prevent another Resendez-Ramirez disaster, for example. As detailed in the state section of this paper, if there had been more openness between the state and national levels there might have been an arrest made prior to a number of the attacks. (National Journal 2000)

There have been multiple illustrations of how this information sharing has proved useful in the past. Virginia and Florida are both states that participate in the DNA databank run by the FBI. In the early 1990s, a criminal named Mark Daigle spent time in a Virginia prison on charges of burglary and grand theft. There were a series of four rapes
in Florida in 1997. The DNA evidence recovered from one of those scenes was run through the FBI banks and it matched the file Daigle had from previously serving time in Virginia. The 31-year-old air conditioning repairman was not even a suspect in the Florida rapes according to the prosecutor, Sarasota County Assistant State Attorney Charlie Roberts. Once the match was made, Sarasota police found that Daigle had been living in the Sarasota area at the time of the assaults and had even lived just down the street from one of the victims at one point. The police had another piece of evidence that further sealed Daigle’s fate – a bloody print at the same scene where the DNA was found. This was matched with the help of Virginia’s database as well. Currently Daigle is in prison for life for one of the rapes and the other three charges await the outcome of his appeal. (Hansen 1999)

Virginia’s laws regarding which criminals have their DNA printed are quite strict; without them Daigle might not have been convicted of the Sarasota rapes. In all actuality, if Virginia, like Florida, only took DNA samples from those convicted of violent or sexual crimes instead of from all convicted felons, “Daigle’s DNA would not have been taken, and we might never have identified him as our rapist,” states Roberts. Because of this Daigle is not at liberty to commit more crimes and therefore, “it’s a good argument for collecting DNA from all convicted felons,” Roberts says. There are additions to the original thought of limiting the sampling to only violent and sexual criminals.

A current article in The National Journal, a judiciary journal (February 2000) looks at the next collection of information that the Justice Department plans to implement. This new network will integrate information from a variety of different
systems -- welfare, health, education, and transportation. This is explained by Paul Kendall, the general counsel for the Office of Justice Programs: "We're seeing that much of the information authorities may need is coming out of education, social services, and other places." The vision held here is that information would travel both vertically (from federal level down to state and local) and horizontally (between states across the country). The common thought is that the more details the officers are armed with, the better they can be at their job. This process is slated to be finished in three to five years, if technological and funding obstacles can be overcome. Technology grants from the Justice Department, of $500 million annually, for the past few years will hopefully build the current systems. This added database of information with its expansive reach and heavy integration will cost hundreds of millions of dollars that has to be appropriated by Congress.

An additional example of the nation's support for this gathering of DNA data is the fact that those entering the military must have their DNA samples taken. This works out to somewhere around 10,000 per day and now should total close to 3.5 million samples collected. The main reasoning behind this is the great help it would be in identifying bodies after an armed conflict when all other options were unavailable. It is simple to see that this trend to compile biological data, which started in the criminal justice system, is becoming more prevalent in our society.
CHALLENGES AND CONCERNS OF A DEMOCRATIC PUBLIC REGARDING A NATIONAL DNA DATABASE

In the democratic society we live in, implementing a national database of DNA information poses many difficulties. We are promised a number of individual rights and protections yet these are not the primary concern of those compiling the DNA data. With the myriad of examples available to show the effectiveness of a localized bank of criminal data, there are also many valid concerns over a system as far-reaching as this one. The technology is certainly available, and has been for quite some time. However, the social and political cultures that must back the use of this database are still problematic. There are plenty of questions and proposals that must be debated before a consensus is reached. While the men and women of law enforcement stand behind the plan for centralized data, the American Civil Liberties Union (ACLU) is one group in opposition to many of the uses that gathering DNA information brings to the forefront. I will attempt to cite a few of these critical concerns that people have raised regarding the implementation of this database.

Public opinion has certainly been mixed on the issue of a national database – it is no longer solely a technological debate but, perhaps more so now, a socio-political one. In our current climate of political distrust, there is a fear of the government having a hidden agenda, or if not this, manufacturing a way in the future to use this information in a harmful way. Jeff Vessels, executive director of the American Civil Liberties Union of Kentucky in 1999, states, “Too often databases are created for one purpose but later used for purposes that are discriminatory and abusive of other peoples’ fundamental rights” (Whitmire 1999). This statement by Vessels is commenting on the way freely given
information, such as nationality, was misused after being gathered from census forms. Statistics, such as population density, were to be gathered to properly appropriate local funding but were certainly not used solely for this purpose in the 1940s. During World War II, Japanese-Americans were rounded-up in internment camps and kept there while they had committed no crime other than admitting they had Japanese blood. A second example, while not quite as unsettling, was the way the assurances over the use of Social Security Numbers were not followed. In the 1930s, citizens were told these numbers would be used only to aid our nation’s pension program. “But over the last 60 years, they have become universal identifiers that they claimed they would not be,” states Barry Steinhardt, associate director of the American Civil Liberties Union. (Byrd 2000)

Certainly these documented cases of government misuse of information or not using data as it was intended are important issues to be debated. The fear is similar to the “Big Brother” idea from the novel 1984; it is thought by many that this is only one additional way for our government to gather more information about us so we can be better monitored. Those who are implementing the databases repeatedly state that this is not the case. They claim they are simply staying abreast of new technology. Law enforcement agencies argue that as criminals become more sophisticated so must the law enforcement agencies whose jurisdictions are being compromised by these “smart crooks.” Gloves are frequently used so fingerprints are not left at a scene and shells are removed before the criminal flees so the ballistics team has little to go on. DNA printing is just another tool to utilize if the other options are made unavailable by the forethought of the culprit. David Coffman, supervisor for the Florida Department of Law Enforcement’s DNA database, is a firm proponent of DNA sampling. “When properly
managed, which the states are doing, this is a valuable tool for fighting violent crime in
the United States,” he said. In the end, it is the capturing of the rapist that may continue
with his crimes that exceeds the need for over-caution in regards to our mistrust of our
government’s future, if yet unrealized, intentions with this sensitive information.

(Colombo 1996)

A second problematic area within the DNA database dispute is the fear of the
unknown. Currently, with the current level of genome technology available, there is
limited DNA information to obtain from criminals other than the random repeats of
“junk” DNA that spell out whether a person is significantly matched to another sample.
However, this DNA science is still young and the technology is constantly changing. It is
a specialized area of science, and the understanding of genes and the way they work is far
from being common knowledge. People distrust what they do not know. Perhaps their
fears are justified in this arena; we are unsure of where technology will lead us in the
future. Today, where we see only “junk,” after ten years of additional studying, we may
be able to discern as much from these chunks of DNA as from the ones that we can
currently read to see propensities for certain diseases.

Critics of this are not convinced. They feel that if samples are kept on file for an
indefinite amount of time, and there is a revolutionary invention in the way we read
DNA, law enforcement can always go back to the samples and extract more relevant
DNA or perform other tests that were not authorized. This criticism runs the other way
as well. If a new technique is invented and there is a need to retest samples and they have
been discarded, it would be nearly impossible in terms of time and money to do a re-
collection of that DNA. There has always been this apprehension about insurance
companies and employers knowing more about us than we would choose for them to know. If the DNA techniques became proficient enough to look at a drop of blood or a strand of hair and see which diseases you are predestined to fall ill to, our current insurance system would become far more selective. (i.e. those who were coded for breast cancer to occur around the age of 35 would have that listed as one of the diseases the company would not cover)

The sampling of DNA is accepted in the field of law enforcement as uniquely effective way of capturing criminals. Because the databases are a newly implemented tool, the debate on the proper uses and controls over DNA has not been settled. It goes without saying that with this new technology a greater number of criminals will be convicted. Yet, if the cost of this is a DNA record of every newborn, are we willing to pay it? I still have the freewill to choose to commit a crime, as crude as that sounds. If I had never been arrested before, my DNA would not be on record anywhere and I would be “free” to go about being a criminal as long as I was intelligent enough to get away with it. Regardless of how wrong it would be for me to commit the crime, I still can do it. If I had my DNA printed as a newborn that freedom would be taken away from me. I think a citizen’s reaction can go both ways in regards to this scenario. Either I approve whole-heartedly in a free society, or I am firmly of the opinion that each and every crime is monitored and solved in due time if DNA evidence is left. A personal decision must be made by each individual to choose which side of the debate one falls on.

The privacy concerns that are encountered when speaking of a complete collection of DNA samples are the final topic I will examine. These concerns are ignored in part when DNA is unwillingly taken or used in ways not condoned by the owner.
Opponents of DNA databases stand firm in the belief that the “benefits of mass sampling don’t outweigh the enormous social costs” (Hanson 1999). The Fourth Amendment to the United States’ Constitution protects against unreasonable search and seizure. Those against the database feel that mass sampling would challenge this law. In 1998, a near-comatose woman at a nursing home in Massachusetts was raped and became pregnant. With no suspects in the case, the Massachusetts police began to take DNA samples from all the men that worked at the home and were ready to issue search warrants for those who refused. ACLU director John Roberts says, search warrants “can’t be a fishing expedition. Just because a person works there doesn’t meet the standard for probable cause” (Adler and McCormick 1998). ACLU officials consider DNA sampling a search under the Fourth Amendment and argue that officials cannot lawfully test, even convicts, without first obtaining a search warrant that sets forth some reason to suspect this particular convict of another, as-of-yet unsolved, criminal activity. Other questions arise in this context as well. Can police demand DNA from people that have been arrested but not convicted? Can police round up people in the vicinity of a crime (i.e. workers in an office building where a crime occurred) and demand their DNA? These sorts of questions are the type that must be answered so the lines are drawn and people know where they legally stand in regards to these issues.

Unlike fingerprinting, DNA is not solely a means of identification. Therein lies the controversy; a DNA sample is akin to holding the blueprint for a particular person. This is a map that might reveal pre-dispositions to illness or other personal facts that we may learn to discern with future study. These privacy advocates fear such a future -- where our government will have the power to commandeer our genetic code, and where
insurance companies and employers may share in the bounty. Taking this forcibly from a person seems to be an issue in need of much contemplation. However, the courts seem to tread carefully around this issue. While failing to make national decrees, rulings in the past of criminals protesting this sampling have tipped heavily in favor of DNA printing. The complaints raised by the ACLU and other like agencies have been virtually ignored. (Hansen 2000) To properly deal with any issue, all the sides must be considered in the beginning to be sure the correct direction is being taken. The common and popular stand of the day is one of "tough on crime" and the courts are skewed toward this point of view as well. The will of the majority should be taken into consideration, but these laws have far-reaching consequences that many database advocates are not aware of. Few are educated in the technology used to sample DNA. Fewer still may have considered the outcomes of laws that may be considered invasion of some of our constitutional rights as Americans.

The other side of the privacy issue is stated succinctly by a North Ohio resident, "I look at DNA just like a fingerprint. It's one of the rights you sacrifice when you commit a crime" (Whitmire 1999). This statement carries some amount of merit, in that, statistics show that over half of offenders will commit another illegal act. (Hanson 1999) This database would decrease the number of those additional crimes that would be left unsolved. One of the realities of prison is that freedoms are taken away as punishment for a crime that did away with the victim's own freedoms. You pay for that violation by losing your freedoms for a particular amount of time. One of these would be your DNA print because this may make it more difficult for you to commit an unidentified crime in the future. There is also the issue of those wrongly accused of a crime and imprisoned.

23
The law could have a clause that calls for the destruction of a sample after innocence is determined. This would only take place in a number of states, however, because in some states (for example, Virginia) the laws regarding sampling are stricter. As a person questioned in a crime, one would be eligible for a sampling to put in the database. One idea that could be used to control those who access the database to view the samples would be to create an electronic audit trail for each person entering the system and to have the system accessed only by a fingerprint reader. In time, there will be regulations determining how samples are accessed and by whom. Until the lines are distinctly drawn in regards to distinct DNA database laws, there are many possibilities to consider when questioning the particular social and political viewpoints of this topic. As stated previously, a personal choice must be made on this issue.
CONCLUSION

In this new age of technology, DNA sampling is going to be used to solve an increasing number of crimes. This fact is met with either great hope and excitement or fills others with dread. There are many concerns in regards to privacy and the fear of the government having our biological data readily accessible.

People still cringe from any hint at our government being an “all knowing” entity; that does not follow the ideals we have set forth in our Democratic society in regards to our leaders. The idea of being tested “kind of goes against an unstated part of the American grain” says Neil McCabe, who studies DNA issues at South Texas College of Law. “When fingerprints first came out, they weren’t accepted – not by the general public and not by the police.” (Higgins 1999) It is generally accepted that sex offenders are sampled but the ordinary citizen’s sample is the point where controversy comes into play. The many examples of crimes solved on both the state and national levels are enough to sway the judgement of some to the side favoring a great deal of sampling. Still others hold the conviction that privacy is too great a thing to have breached – no matter the possible outcomes.

At this point in time we stand at an interesting decision point: the laws regarding DNA testing are still being developed while at the same time the issue remains a relatively unchallenged one by the general public. Our society has the chance to weigh in on these issues before they are decided. The lines have not yet been drawn so speculation is high as to how the government will or should legislate all of this. The FBI seems content to let lawmakers decide the thorny issues (i.e. privacy), still they remain excited about the opportunity to capture criminals similar to those revealed above. This conflict
is sure to be resolved in the near future, because the courts will begin determining which concerns they are willing to address and which need to be cast aside. The decision to choose which side of the debate we on is still available to us. In this light, an understanding of other databases and their uses, a look at the ways the DNA databases can be used for good, and finally a mention of some of the concerns that a grand gathering of biological data means to a democratic society such as ours are relevant and critical issues to our understanding.
BIBLIOGRAPHY


<http://www.redwop.com/minutae.asp?action=showArticle&ID=105>


Callahan, Rick. “Indiana State Police Say Matches Made in 3 Unsolved Cases.” February 2000


Derienzo, Paul and Joan Moossy. “Gene Cops; The Police Want Your DNA.” In These Times: Features Section. December 1999


<http://www.aimsedu.org/activities>


Hansen, Mark. “Banking on DNA: Prosecutors Hail Broadening Collections; Others See Privacy Violations.” ABA Journal: News Section. August 1999

Higgins, Michael. “Acid Test.” ABA Journal: Criminal Justice Section. October 1999


McCullagh, Declan. “DNA Databases Go Too Far.” Wired. April 1999

Niezgoda Jr., Stephan J. and Barry Brown Ph.D. “A CODIS Success Story.”