FORENSICS

THE GOVERNMENT WANTS YOUR DNA

Cops can collect DNA when making an arrest, sometimes before charging a person with a crime. This practice poses a threat to the civil liberties of innocent people

By Erin Murphy

IN BRIEF

Police use of DNA initially posed only a minimal threat to privacy. But collections have expanded to include those arrested for nonviolent crimes and others taken into custody but not yet formally charged with an offense.

DNA sampling has achieved increasing sophistication as police adopt techniques that search databases for samples that only partially match those from crime scenes, a practice that can bring entire families under the spotlight of a criminal investigation.

The U.S. Supreme Court will ultimately decide whether just being arrested for a crime gives police the authority to demand a genetic sample. A variety of legal measures are needed to protect against potential abuses of gargantuan genetic repositories.


EVIDENCE BAG
Name/Rank/No.
Signed

Erin Murphy, professor of law at the New York University School of Law, is an expert on the use of DNA in criminal investigations. Her research focuses on technology and privacy in the criminal justice system, with a particular emphasis on street crime.

STARTING IN THE MID-1980S, A SERIAL KILLER MURDERED at least 10 women in the Los Angeles area. Nicknamed the "Grim Sleeper" because of the long dormancy between his crimes, he eluded capture for nearly 25 years. Then, in 2010, police arrested a man in California for what appeared to be a totally unrelated felony weapons charge. State law required the man to submit a DNA sample for a national DNA database. Typically a DNA database search looks for an exact match between a profile of DNA left at a crime scene by an unknown person and the profile of a known convicted offender. It focuses on 13 places in the genome (the full complement of our DNA) where bits of genetic material vary from person to person. If the crime-scene material differs in any of those 13 places, then the samples do not match, and investigators know that they do not have their suspect.

This time, however, the search was more subtle. It aimed to find DNA profiles that were similar, but not an exact match, to that of the Grim Sleeper. Such an inquiry was possible because in 2008 California became the first state in the nation to formally authorize a new kind of database search. Known as kinship, or familial, matching, this technique looks for partial DNA matches. It is conducted after DNA found at a crime turns up no exact hit. Because related people tend to share more DNA with one another than they do with strangers, a "near miss" in the database may suggest that the search found a person related to the actual perpetrator. Police can then investigate the relatives of the person in the database with the hope of solving the crime.

In the case of the Grim Sleeper, a familial search in 2008 turned up nothing. Two years later, however, the same inquiry generated a lead to the man who had been arrested in California for the weapons offense. Given the fellow's age and the dates of the serial killer's first attacks, suspicion focused quickly on an older relative—his father. A police officer, posing as a waiter at a pizza restaurant, surreptitiously collected genetic samples as the family ate a meal. The sample from the father matched the crime-scene evidence collected long ago, and shortly thereafter the alleged Sleeper was arrested.

This kind of DNA story is so electrifying that television shows like to copy it: a ruthless killer at last outwitted by flashy technology and dogged police persistence. Yet there is another kind of high-tech tale—also about a search for a serial killer—that is equally noteworthy but decidedly disturbing.

Take the case of Shannon Kohler, a Louisiana man approached by officers conducting a DNA dragnet—a broad sweep that netted more than 600 DNA samples from men matching the purported description of the killer. Kohler declined to volunteer a sample but proffered an array of exonerating details, including an accounting of his whereabouts at the time of three of the murders.

Nevertheless, police obtained a court order (later ruled invalid) allowing them to take his DNA and leaked his name to the press—which identified him prominently as a leading and uncooperative suspect in the case. Eventually Kohler's sample established that he was not the murderer, yet authorities never told Kohler of his exoneration. He learned that he had been vindicated only when, two months later, a newspaper printed a small item—after he had endured the dark cloud of suspicion casting him as a potential serial killer and the fear of being wrongly arrested for a capital crime.

As Kohler's saga illustrates, broadening use of DNA testing by law enforcement poses a growing threat to the civil liberties of innocent people. In the 15 years since the national database, called CODIS (*Co*mbined *D*NA *I*ndex *S*ystem), was started, it has amassed DNA signatures of more than 10 million offenders and another 450,000 unidentified people who left genetic material at a crime scene but were never found. The database contains profiles from individuals who have been charged with but never convicted of an offense. More than half of U.S. states now require cops to collect DNA after an arrest for certain offenses.

To address the threat to civil liberties, policy makers should demand answers to simple questions about the precise effectiveness of the technology—for example, finding out how many convictions have come about as a result of DNA database searches

PRECEDING PAGE: GETTY IMAGES

and what percentage of searches turn up useful information—before, as some have suggested, a national database of DNA from everyone in the country is established, allowing any sample collected from a crime to be compared against DNA from the entire U.S. population.

For more than 200 years we have required the police to get a warrant when officers wish to search or seize evidence from individuals in connection with a crime; DNA evidence should be no different. The government should also put in place stricter controls over the use of DNA databases, by taking steps such as forbidding partial matches. Also, it should enact rules to ensure that stored DNA samples are not subject to new tests without court permission and that police databases become available to defense attorneys for exonerating the wrongfully accused. Such changes are not just essential to preserve civil liberties, they are also needed to ensure public safety.

An increasing number of states require that a person provide a DNA sample immediately after being arrested.

THE SLIPPERY SLOPE

AT ONE TIME, the threat posed by compulsory DNA testing was minimal. The practice began in the late 1990s with the passage of state laws compelling people convicted of the most serious felonies, such as murder and sex crimes, to supply blood samples containing DNA. Now these samples are obtained by simply swabbing the inside of the cheek, and the information that is recorded comes from stretches of DNA that vary from person to person but do not reveal anything else about the donor's traits.

In the 2000s states increasingly began to require samples from offenders convicted of less serious felonies or even misdemeanors. Today the federal government and every state mandate compulsory testing of some convicted offenders. Noting that convicted criminals have fewer privacy rights than other citizens, courts have universally upheld such laws.

Yet fresh concerns about civil liberties have been raised by the trend among states in the past five years to require that people arrested for certain crimes give DNA samples. More than half of states and the federal government have arrestee sampling laws in place, some of which authorize the police to take a genetic sample immediately rather than waiting to see if a prosecutor actually files charges. Some states require automatic removal of genetic data collected from a person whose case is later dismissed, but others put the burden on the person wrongly arrested to file a petition to get the DNA record expunged. Finally, some laws provide for the destruction of the biological sample (not just the record), but others allow the government to retain the sample indefinitely.

In the coming months, the U.S. Supreme Court will decide whether DNA samples taken from someone arrested violates the Fourth Amendment of the Constitution. No one disputes that a person arrested for a crime should be required to give a genetic sample if one is needed to compare with evidence found at the alleged scene of the crime. But taking samples from everyone arrested for the sole purpose of expanding the database is a different matter. With more than 14 million arrests annually, a huge fraction of which end in dismissals, arrestee collection statutes could result in many innocent people having their DNA information loaded into police databases and then checked weekly against all the nation's unsolved crimes.

Familial searching, in contrast, has yet to be decided by any court. Like the compiling of arrestee databases, the guidelines for familial searching vary greatly state to state. Yet unlike the rules about whose DNA must go in the database, which are set by democratically elected legislatures, the rules about how police can use the DNA database are often put in place internally by high-level federal or state officials, administrative agencies, or even the heads of individual state or municipal crime laboratories. In fact, the situation is so muddy that it can be difficult even to discern which states engage in what practices. Current data indicate that at least 15 states actively undertake familial searches, although the most prominent users are law-enforcement officials in California, Virginia, Colorado and Texas. Unquestionably, other states have informally conducted occasional searches, and a handful of states are now weighing authorizing legislation. Some states do recognize the potential for abuse. Maryland and the District of Columbia both forbid intentional familial searches by law, and more than 15 states in addition to Maryland prohibit it through written or unwritten policy.

NOT YOUR FATHER'S FINGERPRINT

ADVOCATES of the widespread collection and matching of DNA for crime solving often argue that DNA is no more than a glorified fingerprint and thus raises no new legal issues. Indeed, the handful of courts that have upheld arrestee collection statutes have likened DNA sampling to the routine taking of fingerprints at arrest, a practice long sanctioned by both the courts and the public. Although this analogy has superficial appeal, it is misleading: DNA can potentially provide more information about a person than a fingerprint and can open the door more widely to breaches of privacy.

What is more, even fingerprinting is more invasive than it used to be. Courts have long viewed fingerprinting at arrest as just a minimal encroachment of individual privacy, and for most of the history of the technology it was: a print was taken at a local precinct and then stored in a musty drawer. It was seldom seen again unless police had a new reason to suspect a person of a crime. Today fingerprints, like DNA profiles, are loaded into electronic databases, where they may be automatically searched not just locally but globally. To be sure, access to a common database aids in crime solving. Yet when mistakes occur—and they do happen—the consequences can be shocking. Just remember Brandon Mayfield, the Oregon attorney arrested and held in custody for two weeks as a suspect in the 2004 train station bombings in Madrid because of a faulty fingerprint match.

A false match is the only way to misuse a fingerprint, which simply cannot reveal as much as a person's DNA does. Fingerprints do not tell law enforcement that you have a brother or that you were adopted. They cannot identify you by ethnicity or sex or

reveal whether you are predisposed to cancer. There is no expectation with fingerprinting, as there is with DNA, that it will accurately predict hair and eye color, height, age, bone structure or skin color, not to mention a range of genetic predispositions such as tendencies toward violence, substance abuse or mental illness.

Right now the DNA that is examined and recorded for forensic purposes does not reveal the most personal of these details. But the technology for doing so either already exists or likely will in the future. And the law does not clearly forbid this testing. Courts have consistently interpreted the Constitution to say a great deal about how the police acquire information, but they have exercised very little control over what police then do with that information. If police lawfully obtain a sample, are there then no limits or restrictions on how long that sample can be kept, how long it may be used or what kind of tests can be run on it?

If police examine only DNA fragments that do not reveal personal details, these questions may seem frivolous. Yet because police currently use DNA to make family connections, and in light of ongoing research into using DNA to reveal physical traits, disease and other predispositions, the present legal distinction between the mere acquisition and storage of genetic material and its use for analysis of personal information may quickly turn dangerously antiquated.

DNA crime tech extends beyond futuristic invasions of privacy. Erroneous IDs are more possible than TV crime shows suggest.

It is not hard to imagine that one day police may learn from crime-scene DNA that the unknown criminal is a man of Eurasian descent with blue eyes who is perhaps highly muscular and has a predisposition to alcoholism. Officials may then identify people with a similar profile and investigate those individuals or make their private information public even if many of those under suspicion will end up having nothing to do with the crime. Law-enforcement officials may simply use DNA as a starting point. Information about possible facial characteristics or physical build hinted at through a genetic profile may then be compared against other databases that store photographs of faces and other biometric information, thereby enabling the police to use highly sophisticated and potentially intrusive data mining of personal information on a vast number of the U.S. populace.

The issues raised by the use of DNA technology in law enforcement are not limited to futuristic invasions of privacy or possible harassment of those who happen to be family members of a possible suspect. Even today the potential for mistaken matches is greater than TV crime shows would have you think. The comparison process is far from perfect, especially as smaller and smaller quantities of DNA are tested. Crime-scene samples are generally not in pristine laboratory condition but contain a mix of material from multiple individuals. Analyzing those mixtures is a highly subjective process. One of the few empirical studies of the subjectivity inherent in DNA comparisons recently uncovered alarming possibilities for error: researchers submitted the results of DNA tests in an actual case to 17 experienced analysts; they received significantly divergent reports, ranging from inclusion of the defendant as a possible contributor to the crime to, on the contrary, definitive exclusion.

Finally, one very disturbing aspect of forensic DNA typing is the disproportionate impact that it has on minorities. Because blacks and Latinos make up a greater share of those arrested and convicted in our society, it is their DNA that is most likely to be collected and searched. Yet that is not necessarily because those groups commit more crime. For instance, studies show that across the country, the arrest rate for marijuana possession for blacks and Latinos is double, triple or even quadruple that for whites even though the first two groups do not use marijuana at any higher rate than the third. If police make arrests in a racially skewed way, then DNA databases will also be racially skewed. And it will be those groups whose relatives and family members will be most likely to fall under suspicion as a result of familial-match methods.

The need to more closely regulate law enforcement's use of DNA collection and analysis goes beyond rules and policies related to mandatory collection and familial searches. So far the discussion has centered on the cases in which a person is ordered to give a DNA sample after arrest or conviction. It is also possible, however, for police to obtain DNA surreptitiously, as was done in the Grim Sleeper investigation. In such cases, Fourth Amendment law points in conflicting and often counterintuitive directions. Constitutional protection has traditionally not extended to discarded material—if you throw your bloody shirt in the trash, you cannot complain that your rights were invaded when law enforcement snatches it up as evidence. But should the same reasoning apply to DNA, which is "discarded" routinely, albeit unintentionally? It is simply not possible to live in the world and not shed DNA. Given the myriad ways that DNA can be revealing of intimate personal details, does its ubiquity mean you have no grounds for complaint if the police pick up your discarded soda can and try to match your DNA profile with records in CODIS or store your information in a database or spreadsheet?

FORENSICS OUT OF VIEW

WHAT SHOULD BE DONE to protect the right to privacy of innocent people as DNA use in law enforcement expands? It would be logical to expect that popular sentiment would serve as a check against government abuse of the right to obtain and store DNA from suspects. Yet nearly every aspect of investigative DNA forensics can and does take place behind the scenes, with little public accountability. Investigators have collected samples surreptitiously from people under investigation. New law-enforcement technologies used to analyze those samples are almost always deployed without official comment. Retesting of old samples using new methods happens without prior notice or legal permission. Even government research to determine the effectiveness of DNA methods is shielded from true, scientific peer review. For example, when a list of more than 40 prominent scientists and academics (disclosure: I was among them) published a letter in *Science* requesting controlled access to the national database to verify the accuracy of government claims

about the statistics used to determine how rare certain DNA profiles are, FBI administrators simply refused. The FBI has also threatened to cut off access to states that allow defense attorneys to request to search a government database in an attempt to find the true perpetrator.

The issues that accompany the building of massive DNA databases are only exacerbated by an industry that stands to gain financially from the unchecked embrace of these methods by police and law-enforcement agencies. For-profit companies manufacture the kits used to collect DNA, the instruments required to test it and the software necessary to interpret the results. Private interests benefit every time a new mandatory collection law is passed or a different search technique is approved, especially arrestee laws that will very likely spur demand from every police precinct in the country. It is no coincidence that some of the most vocal proponents of DNA fingerprinting have been employees of lobbying firms promoting their clients' interests, many of whom were previously employed by government labs. For instance, Gordon Thomas Honeywell, a firm that represents Life Technologies, maintains a Web site on legislation aimed at "moving DNA programs forward," and one of the most popular training conferences for law-enforcement analysts is sponsored by Promega, a private technology corporation involved with DNA testing.

NAME, ADDRESS, CHEEK SWAB

STEADY EXPANSION of forensic DNA programs is unlikely to stop with the collection of genetic material from people suspected of crimes or with familial searches. Members of the military are already required to provide DNA samples, although surprisingly, most police officers are not. Soon DNA collection may be considered a reasonable request in exchange for any benefit for which accurate identity is important. Perhaps the government will one day demand a DNA sample from student-loan applicants, government employees, or Social Security or Medicare recipients. And perhaps one day testing will disclose information about more sensitive personal traits.

Some officials and policy analysts have proposed the creation of a population-wide database to which every person would simply contribute at birth. Victim advocates and law-enforcement officials note that a truly national database would go a long way toward solving and controlling crime. Even civil-rights advocates reluctantly note that despite the potential for invasion of privacy, putting everyone's DNA in the ring may be the only way to ensure fairness and accuracy in the use of forensic DNA.

In this age of Google and instant credit checking, of routine bag and body searches at airports, buildings and schools, it is easy to anticipate that our genetic code could soon become just one more piece of currency to trade for a safer society. Yet thin as the line may seem at times, the Constitution has always distinguished between what the government may ask you to do and what it may force you to do.

The Supreme Court has upheld the right of the police to ask you your name, but it has also found that the Constitution prohibits officers from arresting you if you refuse to tell them that information, absent a reasonable suspicion that you were engaged in criminal activity. A threshold has also been set for taking fingerprints: we do not have compulsory national fingerprint programs for crime control. A universal DNA database thus initially strikes legal scholars as patently unconstitutional. If everything short of a population-wide database is on the table, however, how can we best use this powerful forensic tool?

Officials in the U.K. recently answered that question by passing the Protection of Freedoms Act. That law demands the destruction of physical DNA samples taken from arrestees—rather than keeping them for a century, as had been the previous practice—and the purging of innocent persons from the database after a certain period. The U.S. would benefit from similar legislation as well as laws requiring that the efficacy of DNA databases in criminal investigations be evaluated and that rules be put in place to curtail the uses to which biological material collected by law-enforcement officials can be put.

In addition, the government should forbid familial searches that risk casting suspicion on innocent people who have done nothing wrong but are simply related to a criminal offender. At the same time, it should allow access to DNA databases by individuals who are qualified to assess whether the government is abusing this enormous compilation of data. Defense lawyers, too, should be able to search a government database to establish the innocence of a client, as should neutral experts in statistics and population genetics who can check the accuracy of the databases. Laws are also needed to unambiguously clarify which kinds of genetic typing will and will not be allowed—detection of a suspect's physical or personal traits, for instance, might be deemed unacceptable to a society that values civil liberties.

Finally, I would stick to the Constitution's original commitment to freedom from government intrusion into the lives of innocent people by forbidding the indiscriminate taking of DNA samples from anyone arrested. I suggest this step not only out of concern for individual rights but also from a desire to preserve community safety. The tremendous energy directed toward collecting and storing the DNA of arrestees should instead go toward filling an enormous deficit of crime-scene investigators and lab technicians. Emphasis should be on increasing the rate of collection of evidence because as few as 10 to 20 percent of crime scenes for most serious offenses are examined for evidence.

Before the government devotes still more funding to expand its repository of citizen DNA, it should be required to report to the public in detail about the successes achieved so far. We have amassed millions of gene profiles, but no one can say how many arrests have resulted from collecting this information, much less how many convictions or for what offenses. Are these infractions for second-degree murder or merely for marijuana busts? Before we expend more resources and compromise personal liberty still further, we need a concrete accounting—not just anecdotal case reports—of how much the vast investment in DNA collection and recording has already cost taxpayers and society as a whole. SA

MORE TO EXPLORE

The Art in the Science of DNA: A Layperson's Guide to the Subjectivity Inherent in Forensic DNA Typing. Erin Murphy in *Emory Law Journal*, Vol. 58, No. 2, pages 489–512; 2008. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1753906

Relative Doubt: Familial Searches of DNA Databases. Erin Murphy in *Michigan Law Review*, Vol. 109, No. 3, pages 291–348; December 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1498807

SCIENTIFIC AMERICAN ONLINE

Listen to an audio recording of a conference on familial searching at ScientificAmerican.com/mar2013/dna-sampling