AMERICAN CONSTITUTION SOCIETY FOR LAW AND POLICY

A New Era of DNA Collections: At What Cost to Civil Liberties?

By Tania Simoncelli and Sheldon Krimsky

September 2007

A New Era of DNA Collections: At What Cost to Civil Liberties?

Tania Simoncelli[*] and Sheldon Krimsky[**]

On January 5, 2006, a little-noticed piece of legislation entitled the "DNA Fingerprint Act of 2005" was signed into law by President George W. Bush, greatly expanding the government's authority to collect and permanently retain DNA samples.[1] These ninety-nine lines of text, introduced initially by Senator Jon Kyl [R-AZ], slipped virtually unnoticed through the halls of Congress, buried in the back of the broadly popular, 284-page Violence Against Women Act (VAWA) reauthorization bill. Notwithstanding the lack of public reaction and policy debate, this new law raises extraordinary questions for the future of civil liberties. Among other provisions, it grants the government authority to obtain and permanently store DNA from anyone who is arrested as well as non-U.S. citizens detained under federal authorities.

This change in the federal DNA databanking law is emblematic of a new era in forensic DNA – one that is wrought with serious civil liberties and privacy concerns and may ultimately do little to make people safer. While DNA testing was initially introduced into the criminal justice system as a method of developing supplemental evidence to be used in convicting the guilty or freeing the innocent, in the last fifteen years this has changed. The federal government and all fifty states have created permanent collections of DNA taken from ever-widening categories of persons and subjecting these collections to routine searches. At the same time, a stunning array of techniques have emerged allowing lab technicians to glean information from DNA that goes well beyond the mere identification of a person, while the ability to detect and process minute amounts of DNA has steadily increased as costs have declined.

Law enforcement's use of these tools to search, profile and store the DNA of those who have not been convicted of a crime, without a court order or individualized suspicion, has already exceeded reasonable constitutional protections. In particular, a number of new genetic techniques and practices are providing law enforcement unprecedented access into the private lives of innocent persons by way of their own genetic data. These include: 1) a growing trend towards the permanent retention of DNA from innocent people in forensic DNA databanks; 2) trolling for suspects using DNA dragnets; 3) searching for partial matches between crime scene evidence and DNA banks to obtain a list of possible relatives for DNA analysis ("familial searching"); 4) constructing probabilistic phenotypic profiles of a perpetrator from DNA collected at a crime scene; and 5) surreptitiously collecting and searching DNA left behind on items such as cigarette butts and coffee cups.

---

[*] Technology and Science Fellow, The American Civil Liberties Union.
[**] Professor of Urban & Environmental Policy & Planning, School of Arts and Sciences at Tufts University; Adjunct Professor, Department of Public Health and Family Medicine at the Tufts School of Medicine.
[1] The "DNA Fingerprint Act of 2005" was signed into law as Title X of the Violence Against Women Act (VAWA), H.R. 3402, 109th Cong. (2006) (enacted).

This essay explores each of these developments and their implications for civil liberties. We argue that the availability and use of these techniques seriously violates the reasonable expectations of privacy held by law-abiding citizens regarding their DNA. Developing technology, rather than constitutional analysis and informed public decisionmaking, is driving the expansion of DNA databanks. Neglected to date has been a responsible national debate leading to an understanding of the issues and/or resulting in a societal consensus about the variety of uses of DNA discussed in this paper. To help advance the discussion, we urge that policies on DNA-forensic technologies need to calibrate the proper balance of civil liberties and law enforcement needs. We argue that clear national guidelines are needed to set standards for what governmental authorities, as well as private companies and individuals, may and may not do with DNA. We hope to provide a context for re-assessing these and other practices that raise serious civil liberties concerns. Finally, we briefly suggest what some of those guidelines should be.

I. Genetic Privacy

A person's DNA contains a vast amount of information. Those who argue vigorously for collecting and databanking DNA often compare this process to that of collecting and databanking fingerprints. However, fingerprints differ significantly from biological samples that provide DNA. Fingerprints are two-dimensional images of the raised portion of the epidermis of the fingertips. All of the information available from a fingerprint is there to be examined visually once the impression is made of the finger or the copy of the impression left by someone on an object is made. Using the visible individualized characteristics of a fingerprint, it can be used fairly effectively to identify a person. By contrast, DNA, which must be extracted from a tissue sample and mined for data, contains exactly the kind of information that raises privacy and other civil liberties concerns. Research conducted to expand our knowledge of what can be revealed by examining a person's DNA continues; as of this writing, samples of DNA can provide insights into familial connections, physical attributes, genetic mutations, ancestry and disease predisposition. As science advances, the phenotypic information available from human DNA will necessarily grow. Genetic information could be used in discriminatory ways and may include information that the person whose DNA it is does not wish to know. Repeated claims that human behaviors such as aggression, substance addiction, criminal tendency, and sexual orientation can be explained by genetics render law enforcement's collection, use and retention of DNA potentially prone to abuse.

When DNA testing was first introduced into the criminal justice system in the late 1980s, the extent of our knowledge of associations between genes and diseases or other characteristics was quite limited. This changed significantly with the completion of the rough draft of the human genome sequence in 2000 and the final version in 2003. The completion of the project has greatly accelerated research pertaining to the genetic underpinnings of health and disease. Today, clinical testing is possible for more than

1,000 genetic conditions.[2] This illustrates the growing reservoir of information contained in our DNA that would ordinarily be covered under medical privacy statutes.

The highly sensitive nature of the information in our DNA has been widely recognized. For the past two years, the U.S. Senate has unanimously approved legislation that seeks to protect individuals from genetic discrimination in the contexts of employment and health insurance.[3] When introducing the Senate bill on genetic discrimination this year, Senator Edward Kennedy [D-MA] noted, "It is difficult to imagine information more personal or more private than a person's genetic makeup."[4]

The Fourth Amendment of the U.S. Constitution guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[5] The conduct of a "search" generally requires probable cause and a judicial warrant, or at least individualized suspicion.

U.S. courts have consistently found that the collection and analysis of one's DNA constitutes a "search" for two reasons. First, bodily intrusion is necessary for collecting a blood or buccal swab sample for use in DNA testing. Second, the substantial and uniquely personal information contained in the DNA itself has been found to trigger protections guaranteed under the Fourth Amendment.[6] At the same time, though, courts have upheld the operation of convicted-offender DNA databanks – including the forcible extraction and banking of DNA – for one of two reasons: because the government's interest is one of "special needs, beyond the normal need for law enforcement"[7] or because convicted felons have a "diminished expectation" of privacy, as balanced against society's need to promote law and order.[8] Arguably, the role of DNA databanks for convicted felons is for precise identification and for helping police solve recidivist crimes.

Even if these rulings upholding offender databanks (which include biological samples)[9] are correct (and we do not necessarily concede that they are), they do not

---

[2] *See* Genetics and Public Policy Center, *Issue Brief: FDA regulation of genetic tests*, http://www.dnapolicy.org/policy.issue.php (scroll down; follow "FDA regulation of genetic tests" hyperlink).

[3] Legislation to ban genetic discrimination was first introduced in the 104th Congress in 1996. The bill under current consideration is S. 358, the Genetic Information Nondiscrimination Act of 2007, introduced by Senator Snowe. S. 358, 110th Cong. (2007).

[4] 153 Cong. Rec. S847 (2007) (statement of Sen. Kennedy).

[5] U.S. CONST. amend. IV.

[6] *See*, *e.g.*, Jones v. Murray, 962 F.2d 302, 306 (4th Cir. 1992); for a detailed overview of legal challenges relevant to DNA testing and retention, *see* Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127 (2001).

[7] State v. Olivas, 856 P.2d 1076, 1085 (Wash. 1993) (upholding the Washington DNA testing statute, stating that the purpose of the DNA data bank was to deter and prosecute recidivist acts, and that this purpose was a "special need" of government beyond normal law enforcement).

[8] *See*, *e.g.*, Landry v. Att'y Gen., 709 N.E.2d 1085, 1092 (Mass. 1999); *see also* Hudson v. Palmer, 468 U.S. 517, 523 (1984); People v. Wealer, 636 N.E.2d 1129 (Ill. App. Ct.); Jones, *supra* note 6, at 308.

[9] *See* Rothstein & Carnahan, *supra* note 6 (discussing why the special needs exemption may not apply even to convicted offender databanks in light of recent Supreme Court decisions).

provide law enforcement blanket justification to collect and use DNA without limits. As a matter of policy, the notion that innocent individuals should not have DNA taken without their knowledge or consent or retained permanently in a database, or be coerced into providing samples, is reasonable for a society that values freedom and individual privacy. Yet, exactly the opposite is happening, as states and the federal government are giving law enforcement agencies authority to override personal privacy in a technology-driven environment, where the default position seems to be that DNA is open for the taking.

II. The Expansion of Databanks to Include Innocent Persons

Over the past fifteen years, the United States has witnessed a rapid expansion in the banking of DNA for law enforcement purposes.[10] The earliest state statutes, dating back to the early 1990s, limited collection and retention of DNA samples to sexual offenders on the theory that these persons were especially prone to recidivism and most likely to leave behind biological evidence. Successes in linking DNA in some high-profile murder and rape cases combined with an eagerness on the part of politicians to appear tough on crime prompted states to expand their databanks in leaps and bounds. Today, forty-five states collect DNA from all felons, thirty-two from juvenile offenders and thirty-four from those who commit certain categories of misdemeanors.

Congress enacted the "DNA Identification Act of 1994" authorizing the FBI to maintain a centralized, national DNA database and to develop a software system to allow for the sharing of information within and between the states. By 2004, the resulting system – the Combined DNA Index System (CODIS) – connected the databases of all fifty states, which at that time were limited to profiles from those convicted of serious, violent crimes. Signed into law by President George W. Bush on October 30, 2004, the "Justice For All Act" (P.L. 108-405) greatly expanded the CODIS system, allowing collection of DNA from all federal felons and enabling states to upload to CODIS profiles from *anyone* convicted of a crime.

In the last few years, enthusiasm for DNA banking has prompted some state legislatures to expand their databanks beyond convicted offenders to innocent people – both those presumed innocent until proven guilty and those who are actually innocent. Eleven states – Virginia, Texas, Louisiana, California,[11] New Mexico, Minnesota, Kansas, Tennessee, North Dakota, Alaska, and Arizona – have approved legislation to allow DNA testing of some categories of arrested individuals [see Table I]. Tennessee recanted its expanded databank provisions when it proved too costly to hire the six

[10] *See* R. Weiss, *Vast DNA Bank Pits Policing Vs. Privacy*, WASH. POST, June 3, 2006, at A01; *see also* Jonathan Kimmelman, *The Promise and Perils of Criminal DNA Databanking*, NATURE BIOTECHNOLOGY, July 2000; Tania Simoncelli, *Dangerous Excursions: The Case Against Expanding Forensic DNA Databases to Innocent Persons*, 34 J.L. MED. & ETHICS 390 (2006).

[11] For a detailed analysis of California's Proposition 69, *see* Tania Simoncelli & Barry Steinhardt, *California's Proposition 69: A Dangerous Precedent for Criminal DNA Databases*, 33 J.L. MED. & ETHICS 279 (2005).

additional DNA analysts needed to process arrestee samples,[12] but reauthorized arrestee testing for a narrower group of individuals in the subsequent legislative session. Last year, Minnesota's Court of Appeals held that taking DNA from juveniles and adults who have had a probable cause determination on a charged offense but who have not been convicted violates state and federal constitutional prohibitions against unreasonable searches and seizures.[13] As a result, currently a total of ten states allow for the collection and retention of DNA from persons who are arrested.

Some states have gone even further and have started to retain DNA from people identified as "suspects." For example, California's Proposition 69, adopted by voters in 2004, allows DNA taken from suspects to be retained for up to two years and compared "in and between, as many cases and investigations as necessary, and searched against the forensic identification profiles, including DNA profiles, stored in the files of the Department of Justice DNA data bank or database or any available data banks or databases as part of the Department of Justice DNA Databases and Data Bank Program."[14]

Where their statutes do not authorize or allow it, some state law enforcement agencies have proceeded to collect and bank DNA anyway, creating "offline" databanks that contain DNA from arrestees, suspects, people caught up in "DNA dragnets," bystanders at a crime scene, and victims and their partners. Thus far, such "offline" databanks have been discovered in Louisiana and New York.[15] In these instances, law enforcement appears to be operating the databanks without authorization or oversight, and samples are being subjected to searches and retained indefinitely without the informed consent of the individuals who provided them.[16]

At the federal level, the DNA Fingerprint Act of 2005 was signed into law in January 2006, authorizing DNA collection and retention from persons arrested or non-

---

[12] Offender DNA Database Expansion: 2006 Legislation, http://www.dnaresource.com/documents/2006DNAExpansionbills.pdf.

[13] In re Welfare of C.T.L., 722 N.W.2d 484 (Minn. Ct. App., 2006).

[14] "DNA Fingerprint, Unsolved Crime and Innocence Protection Act," Cal. Proposition 69, Section III, Article 3(b)(1) (initiative measure to be submitted directly to voters), *available at* http://www.sos.ca.gov/elections/bp_nov04/prop_69_text_of_proposed_law.pdf.

[15] Barry Scheck, Co-Director, The Innocence Project, DNA Databases, A Panel Discussion at the ACLU Forum on Technology and the Future (Oct. 22, 2006).

[16] A lawsuit is pending in the state of New York that challenges the legality of an offline databank that is being maintained by the New York Medical Examiner's Office. An amicus brief filed by the Innocence Project and the New York Civil Liberties Union asserts that the "linkage database" is inconsistent with state law, which requires expungement of DNA samples from individuals who are acquitted or whose conviction is subsequently reversed on appeal or vacated. It argues that the databank violates Fourth Amendment limitations that prohibit seizures beyond the initial purpose for which the seizure took place and that the database violates Fourteenth Amendment rights of informational privacy and individual autonomy with respect to the use and maintenance of one's DNA. *See* Brief for the New York Civil Liberties Union and the Innocence Project as Amici Curiae Supporting Defendant, People v. Hendrix, Indictment No. 3668/03 (N.Y. App. Div. Dec. 30, 2004).

U.S. persons detained under federal authority.[17] Under this law, the Attorney General is given broad discretionary power to grant DNA testing authority to any federal agency.[18] The new law also allows states to upload any profiles that are collected under "applicable legal authority," so long as voluntarily submitted samples are not included.[19] This broad mandate, which does not define "applicable legal authority," potentially gives any law enforcement agency at any level of government the right to upload DNA profiles of any individual, including juveniles for minor misdemeanors, whether the DNA was taken by warrant, by demand or surreptitiously.

The DNA Fingerprint Act not only gives federal imprimatur to arrestee testing, it provides direct financial incentives for states to expand their databanks accordingly by broadening the eligibility requirements associated with a federal grant program that supports DNA testing to include arrestees.[20] This year, legislative proposals to expand DNA collections to some categories of arrestees were introduced in twenty-five states (as compared with only nine states in 2006, and eight states in 2005).[21]

Proposals are being considered to expand databanks to other categories of innocent persons, including the vast majority of people who are suspected of no crime whatsoever. Following 9/11, some suggested incorporating DNA collection into the U.S. visa application process. Appealing to notions of "fairness," others have suggested taking DNA databanking to the extreme, calling for the government to simply place everyone in the nation and their DNA in the database. Last year, Prime Minister Tony Blair called for such a database for the United Kingdom.[22] Proposed collection methods for such a universal database include linking law enforcement with state newborn screening programs,[23] taking samples when children are vaccinated for entering school,[24] making a DNA sample a requirement for obtaining a driver's or marriage license[25] and

---

[17] The DNA Fingerprint Act of 2005, S. 1606, 109th Cong. § 1004(a)(1)(A) (2005) ("The Attorney General may, as prescribed by the Attorney General in regulation, collect DNA samples from individuals who are arrested or from non-United States persons who are detained under the authority of the United States").
[18] *Id*. ("…The Attorney General may …. Authorize and direct any other agency of the United States that arrests or detains individuals or supervises individuals facing charges to carry out any function and exercise any power of the Attorney General under this section").
[19] The DNA Fingerprint Act of 2005 maintained the restriction in the law that requires that "DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System." *See* 42 U.S.C. § 14132 (a)(1)(C) (2005).
[20] *See* U.S.C. 42 §14135 (a)(1) (2005), *amended by* The DNA Fingerprint Act of 2005, S. 1606, 109th Cong. § 1003 (2005).
[21] Legislation to expand DNA collection to certain categories of arrestees has been introduced in the following states in 2007: Alaska, Arkansas, Arizona, Connecticut, Hawaii, Idaho, Indiana, Illinois, Maryland, Michigan, Mississippi, Missouri, Montana, New Jersey, North Dakota, New York, Oklahoma, South Carolina, and Tennessee.
[22] George Jones, *DNA Database 'Should Include Al,'* TELEGRAPH NEWSPAPER, Oct. 24, 2006, *http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/10/24/ndna24.xml.*
[23] *See* D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413 (2003).
[24] *See* Rebecca Sasser Peterson, *DNA Databases: When Fear Goes Too Far*, 37 AM. CRIM. L. REV. 1219, 1228 (2000).
[25] *Id*.

creating a national identification card that incorporates DNA information.[26] Notably, all of these methods of collecting DNA for law enforcement purposes are unrelated to the purposes for which people are otherwise interacting with the State.

The trend to collect and bank the DNA from innocent persons including newborns, schoolchildren, suspects and arrestees is highly problematic. First, it marks a fundamental shift in the purpose and intent of what have been termed "criminal" databanks. The routine trawling of these databases by law enforcement renders the people whose personal data are included as suspects for any and all future crimes even though they have not actually been deemed suspects by any method. Requiring persons convicted of a crime to forfeit certain rights of bodily integrity and privacy while under authority of the penal system has been ruled defensible. However, subjecting those who have *never* been suspected of a crime, let alone convicted of one, to this treatment potentially undermines the presumption of innocence. Adding the DNA data from millions of innocent persons to these databanks alters their purpose from one of criminal investigation to population surveillance, subverting our deepest notions of a free and autonomous citizenry.

Furthermore, there is no reason to assume that biological samples and DNA data in the hands of the government would be safe from misuse, or that all purposes for which it may be used will be either appropriately law-enforcement related or benign. The privacy concerns associated with potential misuse of DNA information are driven by current laboratory practice, where the individual's biological sample is retained along with the generated profile. Since all of our genetic information is encoded in each and every one of our cells, the risk of abuse remains real as long as the biological samples remain on file. Only one state – Wisconsin – mandates the destruction of the individual offender's biological sample after a DNA profile is generated,[27] although to date, none has been destroyed. Twenty-nine states specifically require retention of the offender samples.

State databank statutes vary on issues of expungement, although the general trend is one of placing the burden on the individual, rather than the state, to expunge the DNA profile and destroy any biological samples upon proof of innocence or a reversal of charges. Under Proposition 69, for example, a Californian who is no longer a suspect for a crime or whose DNA is inadvertently placed into the database has to file a written petition with three separate agencies in order to have their DNA-related information expunged.[28] When a request for expungement is denied it is unappealable and thus lacks procedural safeguards.[29]

---

[26] *See* Ben Quarmby, *The Case for National DNA Identification Cards*, 2003 DUKE L. & TECH. REV. 2 (2003).
[27] *See* Seth Axelrad, *Survey of State DNA Database Statutes* (2004), http://www.aslme.org/dna_04/griod/guide.pdf.
[28] "DNA Fingerprint, Unsolved Crime and Innocence Protection Act," Cal. Proposition 69, Section III, Section 9, *available at* http://www.sos.ca.gov/elections/bp_nov04/prop_69_text_of_proposed_law.pdf.
[29] *Id*.

Some states have also explicitly allowed their databases to be used for a variety of non-law-enforcement purposes. For example, Massachusetts law allows for the disclosure of DNA records for "advancing other humanitarian purposes." Alabama's statute allows its database to be used to "provide data relative to the causation, detection and prevention of disease or disability" and to "assist in … educational research or medical research or development."[30]

Allowing research on law enforcement databanks is deeply troubling. An association found between a genetic mutation and violence – whether real or perceived – could be used as a means for attempting to screen out violent offenders before they strike. Recently, a bill was introduced into Congress to create a separate DNA database of all violent predators against children.[31] While not stated explicitly, one has to wonder if the impetus behind separating out the DNA of these offenders is to conduct research on this particular population. Certainly such a database would be a goldmine for a behavioral geneticist who might be interested in studying the genetics of pedophilia or violence against children, if they indeed even have a genetic component. Credible studies in behavioral genetics can contribute to useful knowledge, but they must follow the principles of the Common Rule, which requires informed consent from anyone whose DNA is being used.

From one legal perspective, it is hard to see how the inclusion of sensitive personal data on large numbers of innocent people in a government databank could pass constitutional muster. Yet, as shown, in cases where convicted offender DNA databanks have been challenged on the grounds of the Fourth Amendment, the courts have generally upheld the databanks for one of two reasons: because the government's interest is one of "special needs, beyond the normal need for law enforcement;"[32] or because convicted felons have a "diminished expectation" of privacy.[33] A number of scholars have noted that the application of the "special needs" exception to DNA databanks is questionable, given two recent Supreme Court rulings. In *City of Indianapolis v. Edmond* and *Ferguson v. City of Charleston,* the Court found that where the primary purpose of a program involving a search is related to the general interest in crime control, the "special needs" exception under the Fourth Amendment does not apply; in that circumstance a warrant supported by probable cause is required.[34] Similarly, while it is plausible that the

---

[30] ALA. CODE § 36-18-31 (2007).

[31] Save Our Children: Stop the Violent Predators Against Children DNA Act of 2007, H.R. 252, 110th Cong. (2007).

[32] *See* State v. Olivas, *supra* note 7 (stating that the purpose of the DNA data bank was to deter and prosecute recidivist acts, and that this purpose was a "special need" of government beyond normal law enforcement).

[33] *See*, *e.g.*, Landry v. Att'y Gen., *supra* note 8; *see also* Hudson, *supra* note 8; People v. Wealer*, supra* note 8 ; Jones, *supra* note 8.

[34] *See* City of Indianapolis v. Edmond, 531 U.S. 32 (2000) (striking down a program in which police used dogs to sniff for drugs in vehicles pulled over in groups at fixed roadblocks because they found the primary purpose of the checkpoint program to be related to the general interest of crime control); *see also* Ferguson v. City of Charleston, 532 U.S. 67 (2001) (striking down a program in which a university hospital tested urine samples from pregnant women for cocaine and reported positive results to the police because the primary purpose of the program was said to be the arrest and prosecution of drug-abusing mothers, and therefore of the general interest of crime control).

courts could uphold the forcible taking and analysis of DNA of persons arrested on the basis of some diminished expectation of privacy while in confinement, the permanent retention of that DNA probably cannot be justified on this basis unless a suspect is convicted of a crime.

The Court of Appeals in Minnesota followed this logic in overturning Minnesota's arrestee testing law. Affirming the district court's opinion, the appeals court held that statutory provisions directing law enforcement to take biological specimens from juveniles and adults who have had a probable cause determination on a charged offense but who have not been convicted, violate state and federal constitutional prohibitions against unreasonable searches and seizures. In particular, the court found that the state's interest in collecting and storing DNA samples is outweighed by the privacy interest of a person who has not been convicted.[35]

III. Trolling for Suspects: The Use of DNA Dragnets

In 1987, British Authorities in Leicestershire Township decided to try something that neither they nor any other police department had previously undertaken. Upon coming to a dead end in the investigation of a double rape-murder of two 15-year-old girls, they initiated an aggressive outreach program in which voluntary blood and saliva samples were requested from all unalibied male residents between the ages of 17 and 34 in the neighboring villages of the crime. While the perpetrator was not one of the 4,000 individuals from whom DNA was actually collected, he was eventually caught when he was overheard attempting to persuade a friend to submit a sample on his behalf.

Since this initial "success" case – which was not actually a success in terms of identifying a suspect of a crime from DNA data collected – the "DNA dragnet" has become a new method for investigating crimes where the police have not had success obtaining leads using traditional law enforcement measures. When a crime scene has tell-tale forensic DNA evidence (blood, semen, hair follicles and/or saliva) that is suspected (although not known) to have been left by the perpetrator, the DNA dragnet seeks to obtain samples from large numbers of people who live or work in the vicinity of the crime scene or fit a loose profile of the perpetrator. In these cases, police investigators round up hundreds if not thousands of individuals and ask them to "voluntarily" provide a DNA sample. Following the experience of the UK, at least nineteen American cities and towns in the United States have undertaken DNA dragnets, some of them involving thousands of people.[36]

DNA sweeps raise profound civil liberties concerns because they involve the government collecting DNA from people for examination without probable cause. In addition, the claim by law enforcement that dragnets are truly "voluntary" has been widely criticized; for example, declining to "volunteer" has left individuals subject to

[35] In re Welfare of C.T.L., *supra* note 13.
[36] *See* Department of Criminal Justice, University of Nebraska at Omaha, Police DNA 'Sweeps' Extremely Unproductive, a report by the Police Professionalism Initiative (Sept. 2004).

social stigmatization or coercion or forcible collection of their DNA.[37] During a DNA dragnet in Oklahoma in 2001, individuals who refused to consent to DNA testing were served with search warrants and treated as suspects.[38] In Louisiana, a man who refused to provide a sample to police was threatened that a court order would be issued, and that his name would be reported to the press.[39] Steven Turner, a 27-year-old University of Virginia graduate student, was stopped by the police while he was riding his bike, because he allegedly fit the profile of a 6-foot black man in his early 20s with an athletic build and "unnaturally white, bulging eyes." [40] When he refused to give police a cheek swab, two officers showed up at his home. Even as police assured Turner that he would be eliminated as a suspect in the crime if he complied, he refused to supply his DNA. After black community leaders complained to the Charlottesville police chief, police ceased requesting cheek swabs from black men simply because they look suspicious or resemble a police sketch of the rapist.[41]

In some cases, even after individuals are cleared of the crime in question, they have not been able to get their DNA back. At least two lawsuits – one in Michigan[42] and one in Louisiana[43] – have arisen from denied requests to have DNA returned to individuals who have "volunteered" their DNA. The discovery that authorities in Louisiana and New York have been maintaining "offline" databanks begs the questions of whether thousands of other individuals around the country have had their DNA retained, illegally or at least without express authority, and compared with evidence from crime scenes. Unless checked by strict guidelines and monitored by independent groups, police dragnets can become intolerably coercive. For example, it has been authoritatively noted that, "[a]lthough consent to participate in a dragnet is normally voluntary, such requests from law enforcement officers are inherently coercive."[44]

IV. Using DNA to Create Suspects Out of Family Members

"Familial searching" of databases is another new method of creating suspects in the absence of an immediate "cold hit." "Familial searching" is premised on the notion that siblings and other closely related individuals share more common genetic material than non-related individuals. Current methods of familial searching involve generating a list of possible relatives of the owner of DNA picked up at a crime scene by performing either a "low stringency" profile search to look for "partial matches" between crime scene evidence and offender profiles or by conducting a "rare allele" search. Close

---

[37] *See* Mildred K. Cho & Pamela Sankar, *Forensic Genetics and Ethical, Legal and Social Implications Beyond the Clinic*, 36 NATURE GENETICS 8 (2004).
[38] *DNA Dragnets*, 8 THE NEW ATLANTIS 104 (2005).
[39] Glynn Wilson, *In Louisiana, Debate over a DNA Dragnet*," CHRISTIAN SCIENCE MONITOR, Feb. 21, 2003, *available at* http://www.csmonitor.com/2003/0221/p03s01-usju.html.
[40] Lorraine M. Blackwell, *Virginia U. Suspends DNA Dragnet Locating Serial Rapist*," THE DAILY TEXAN, May 4, 2004.
[41] *Id*.
[42] *See* Shelton v. Ann Arbor Police Dep't., 568 N.W.2d 87 (Mich. 1997).
[43] *See Men Targeted by 'DNA Dragnet' Demand Return, Destruction of Samples*, THE NEW STANDARD, Nov. 9, 2004.
[44] Mark A. Rothstein & Meaghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?*, 34 J.L. MED. & ETHICS 153 (2006).

relatives of those matches are then tracked down and asked to "voluntarily" provide a DNA sample.[45]

In 1973, three women were murdered in South Wales. Twenty-nine years after the crimes were committed, the police submitted crime-scene stains to the United Kingdom's National DNA Database (NDNAD). When no full matches were found, a low stringency analysis indicated that the DNA partially matched the DNA profile of a man named Paul Kappen. Police surmised that someone in Kappen's family was the murderer, leading them back to Paul Kappen's father, Joseph, who had already died. British law enforcement authorities obtained DNA samples from the Kappen family, including Paul Kappen's mother and his siblings. The close match between the crime scene and family DNA profiles was sufficiently credible for the police to obtain a warrant to exhume the body of Joseph Kappen. His DNA was an exact match with the crime scene DNA. The case was solved by familial searching posthumously.

Familial searching has been employed in the United Kingdom in at least twenty criminal investigations.[46] In the United States the practice was quite limited until recently by a policy adopted by the FBI prohibiting the release of any identifying information about an offender in one state's database to officials in another state unless the offender's DNA was an exact match with the DNA evidence found at the scene of crime. Last summer, however, the FBI changed its policy in response to a request from Denver authorities who found a close match between evidence taken from the scene of a rape and a convicted felon in Oregon, indicating that he was a potential relative of the actual perpetrator. The interim policy, effective July 14, 2006, allows for states to share information related to "partial matches," upon FBI approval.[47] This has opened up the floodgates for using CODIS in conjunction with familial searching.

Familial searching raises a series of potentially troubling civil liberties issues. First, if practiced routinely, it effectively expands the database to a whole new category of innocent people whose private genetic data may be mined even though they themselves are not suspects in any criminal case – those who happen to be relatives of convicted offenders or others whose DNA data is kept in government databases. Family searches may also reveal information that family members prefer to keep private; for example, an offender might name someone as a parent or child who turns out to be genetically unrelated to them.

In addition, there are a host of unanswered procedural questions associated with how the police might follow up on leads provided by partial matches. A low stringency

---

[45] *See* Frederick R. Bieber, *Science and Technology of Forensic DNA Profiling: Current Use and Future Directions*, *in* DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE (David Lazer ed., 2004); *see also* Ben Mitchell, *Police Warning to Criminals over DNA Breakthrough*, THE SCOTSMAN, Nov. 19, 2004.

[46] Robin Williams, Making Do with Partial Matches: DNA Intelligence and Criminal Investigations in the United Kingdom, Presentation for DNA Fingerprinting and Civil Liberties: Workshop #2, American Society for Law, Medicine & Ethics (Sept. 17, 2004).

[47] FBI, CODIS Bulletin, Interim Plan for the Release of Information in the Event of a Partial Match at NDIS (July 20, 2006).

search (generally defined as a match of 8-12 alleles out of the usual 13-15) can generate tens, hundreds, or even thousands of partial matches (and these will continue to grow as the databases grow). A partial match only indicates that there is some possibility that a relative of that person could have DNA that fully matches the crime scene evidence – the probability that the partial match is useful depends both on the number of alleles that are found to match, and their respective rarity in the population. As such, the police might be tempted to knock on the doors of hundreds or thousands of individuals, in the event that they do not have further evidence to narrow down their initial list of partial matches. Assuming that a partial match is not sufficient evidence for compelling a relative to provide a DNA sample via a court order, what happens if those individuals refuse to provide a sample? What is the fate of the samples collected? Will they be destroyed if that person is excluded from the crime? Will there be a temptation on the part of law enforcement to follow people around to get their DNA surreptitiously, when a court warrant cannot be obtained because there is insufficient evidence of individual suspicion?

V. Phenotypic DNA Profiling

In an even more disturbing trend, some law enforcement agents have tried to construct phenotypic profiles of the suspected perpetrator based on analyses of the DNA found at a crime scene.[48] In a murder investigation in Louisiana, for example, a relatively new method of DNA analysis was employed to predict the "ancestry" of the alleged offender as 85% Sub-Saharan African and 15% Native American. The company that performed the analysis, DNAPrint Genomics, has been aggressively marketing the service to police departments, investigators and agencies.[49] The company has also recently started offering to law enforcement agencies a genetic test to infer eye color.[50]

A blood stain left at a crime scene could be subjected to many other tests, including any of the 1,000 plus tests for genetic conditions that are currently available. Law enforcement might use this information in an attempt to narrow down a pool of suspects. For example, suppose a blood stain were sent off to a private lab and the lab ran a battery of genetic tests and found that the DNA of the stain contained the two genetic mutations associated with Gaucher disease, a metabolic disorder that causes a buildup of fatty substances in the spleen and liver and results in fatigue and bruising easily. Law enforcement might then try to get a list of names of all of the people receiving enzyme replacement treatments for Gaucher at the neighboring hospital. Would they be given those names? Under what circumstances? Do people then become suspects for a crime simply because they might have a pre-disposition to a certain health condition?

---

[48] *See* Nita A. Farahany & William Bernet, *Behavioral Genetics in Criminal Cases: Past, Present and Future*, 2 GENOMICS, SOC'Y & POL'Y 72 (2006).

[49] *See* Press Release, DNAPrint Genomics, Inc., DNAPrint Genomics Is Encouraging Law Enforcement Agencies To Include DNAWitness ™ In Their NIJ Grant Proposals, available at http://www.dnaprint.com/welcome/press/press_recent/2004/august_16/ (Aug. 16, 2004).

[50] *See* Press Release, DNAPrint Genomics, Inc., DNAPrint Announces The Release Of RETINOME™ For The Forensic Market: Eye Color Prediction From Crime Scene DNA, available at http://www.dnaprint.com/welcome/press/press_recent/2004/august_17/ (Aug. 17, 2004).

Under the Health Insurance Portability, Accountability Act (HIPAA), a person's DNA information and tissue samples are protected. However, HIPAA contains a broad exception that allows for disclosure of Protected Health Information to law enforcement officials, not only in compliance with a court order or grand jury subpoena, but also in response to an administrative subpoena, summons or civil investigative demand. It is worth noting that all of these are legal instruments issued without judicial review.[51] Broad administrative discretion is given to those with stewardship over health information at the hospitals in determining how to respond to written requests from law enforcement for patient records. HIPAA also allows health care providers to disclose to law enforcement, upon request, a broad array of identification information, including name, address, social security number, blood type, date of treatment and a physical description. Federal HIPAA guidelines should be tightened to protect the privacy of medical information, especially in cases where court warrants are not issued, to insure uniformity in the interpretation of the policy.

There is also an obvious temptation on the part of law enforcement to mine crime scene DNA to make predictions about the physical, behavioral or medical conditions of the alleged perpetrator that will likely increase over time. Already, claims have been made that genetic factors have been found that are associated with sexual orientation, intelligence, addictive behavior and aggression. Even if they are unsound, law enforcement will be tempted to use them so as to generate profiles of suspects from the DNA, such as: "Likely to be a tall, African American homosexual male, with high intelligence, a propensity for addiction, and recessive for sickle cell anemia." Even if there were reliable population-wide probabilistic inferences from genotype to phenotype, confounding factors would make these inferences questionable for any individual.

This trend is likely to continue with the advent of gene chips, or DNA microarrays, such as those that have been developed by the company, Affymetrix.[52] These gene chips allow researchers to access information on thousands of genes simultaneously. At the same time, scientists have developed DNA sequencing devices as small as 10 cm in diameter[53] while the "Personal Genome Project seeks ultimately to make it affordable for people to sequence their own, individual genome.[54]

VI. Surreptitious DNA Collection

In 1974, a woman was raped and stabbed in Buffalo, New York. A few weeks ago, a 60-year-old man was arrested and charged with the crime. The police did not have

---

[51] *See* Rothstein & Talbott, *supra* note 6; *see also Law Enforcement Exemptions to the HIPAA Regulations: Testimony Before the Subcomm. on Privacy and Confidentiality of the National Comm. on Vital Statistics* (Feb. 18, 2004) (statement of Chris Calabrese, Counsel to the American Civil Liberties Union's Technology and Liberty Program).

[52] Affymetrix, http://www.affymetrix.com/index.affx.

[53] *See* Bioengineers develop smallest DNA sequencer (May 9, 2006), http://bioeng.berkeley.edu/content/view/307/157/.

[54] *See* Emily Singer, *The Personal Genome Project*: What Would Happen if Genetic and Medical Records were Freely Available to Anyone who Wanted Them?, TECH. REV., Jan. 20, 2006, http://www.technologyreview.com/Biotech/16169/.

enough evidence to obtain a warrant for his arrest. Instead, they followed him around, picked up his DNA after he spat on the sidewalk, and compared it to the 30-year-old crime scene sample.[55]

This is the latest of an increasing number of known examples where police have collected DNA from individuals surreptitiously and without warrants supported by evidence amounting to probable cause. In another case, the police employed a ruse in order to get their suspect, John Athan, to provide them with a DNA sample. Posing as a law firm, the police sent Athan a letter, asking him to join a lawsuit aimed at recovering overcharges in traffic fines. When they received a return letter from him, they lifted his DNA from the dried saliva where he had licked the envelope. The Washington State Supreme Court affirmed Athan's conviction, finding no Fourth Amendment violation by police conduct.[56]

These cases beg the question: What does it mean to live in a world where one has to assume that DNA shed on a continual basis might at any time be picked up, extracted and analyzed for information that could lead to one's arrest or conviction, to behavioral profiling or to the even more-attenuated identification of family members as crime suspects?

The primary argument asserted by law enforcement to justify surreptitious DNA searches is that the DNA is "abandoned."[57] In other words, an individual who "abandons" her DNA no longer has any privacy interest in that DNA.

This argument is problematic on a number of counts. First, "abandoned" implies a knowing intent to part with an item. People abandon items they no longer wish to own or carry around. But DNA is not so much abandoned as it is inadvertently and continually shed from people's bodies in the form of skin cells, saliva and hair samples. Short of walking around in the world in a plastic bubble suit, it would be virtually impossible to refrain from shedding DNA.

Shedding DNA is not like leaving garbage at the curb. When people leave garbage on the street, they have come to anticipate that someone might rummage through it. They expect that the private information that might be contained in letters or bills can be accessed virtually by anyone who might come into contact with that garbage, which is why many people choose to shred key papers. However, DNA cannot be "read" or even seen unless it is collected and then subjected to sophisticated, expensive equipment. The privacy interest associated with DNA comes into play not in the form in which it inadvertently left the body, but instead when it is analyzed for the microscopic

---

[55] *See* Carolyn Thompson, *Police DNA Collection Sparks Questions*, ASSOCIATED PRESS, March 17, 2007, http://www.usatoday.com/news/nation/2007-03-17-dna-collection_N.htm?csp=34.

[56] *See* Brief for American Civil Liberties Union of Washington as Amici Curiae Supporting Defendant, State v. Athan, 158 P.3d 27 (Wash. 2007); *see also* Richard Willing, *Police Dupe Suspects into Giving up DNA*, U.S.A. TODAY, Sept. 11, 2003, at A03.

[57] For a detailed analysis of the concerns associated with the collection of so-called "abandoned" DNA, *see* Elizabeth E. Joh, *Reclaiming 'Abandoned' DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006).

information contained therein. And certainly there is no mechanism for "shredding" the DNA that continuously gets released from the human body.

Police point to individual success stories in solving crimes as a way of justifying surreptitious DNA collection as a "clever investigation technique." But allowing police to take DNA without a person's knowledge or consent opens the door to mass DNA collections of anyone vaguely suspected, or even to those who are perfectly law-abiding and suspected of no criminal activity. Individuals would have no way of contesting this collection or use of their DNA. This scenario becomes increasingly worrisome when coupled with developments in behavioral genetics; weak or unreliable genetic markers for aggression or addiction could provide justification for identifying individuals who, it is believed, will commit a crime, and placing them under surveillance or social control.

VII. Expanding Databanks and the Efficacy of Solving Crimes

The techniques and practices discussed above go a good distance to undermine the privacy of individuals. At the same time, it is possible that people are being asked to sacrifice their privacy for a process that may ultimately do little for criminal justice. In the case of the databanks, while law enforcement tends to boast large numbers of "cold hits" or "investigations aided," so far there has not been a single, peer-reviewed study that demonstrates the true effectiveness of the databanks.[58] While the prevailing notion with respect to these databanks is "the bigger the better," it is worth noting that the ability to use DNA in crime solving is limited by the ability to collect uncontaminated and undegraded DNA at a crime scene, not by the number of people in the databank. As the databanks expand to people convicted of minor offenses or merely arrested, the chances that any given profile in the database will help resolve a future crime apparently diminish. In the United Kingdom, the enactment of arrestee testing in 2004, which has corresponded with a ballooning of the UK database from 2 million to 3 million profiles (including those of more than 125,000 people never charged any crime), has actually corresponded with a slight *decrease* in matches with crime scene evidence.[59]

Likewise, DNA dragnets have proven to be highly ineffective. In a study conducted by the University of Nebraska, only one of eighteen dragnets conducted in the United States was found to have led to the actual perpetrator, and this was a dragnet that only involved 25 people who were all staff at a nursing home where repeated sexual offenses were taking place.[60] In other words, the obvious small pool of suspects already existed. Worse still, some dragnets have even been found to interfere with crime-solving. Police had for well over a year the DNA of the individual who was ultimately charged with the murder of Cristina Worthington. The DNA had not been tested, however,

---

[58] *See* Rothstein & Talbot, *supra* note 49.
[59] *See* GeneWatch UK, *The Police National DNA Database: An Update,* Human Genetics Parliamentary Briefing No. 6, (July 2006) (*available at* http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/MPSBrief_1.pdf).
[60] *See supra* note 41

because law enforcement officials were busy collecting DNA from some 1,000 innocent individuals[61] in hopes of using that DNA to solve the crime.

In the case of familial searching, it is perhaps too soon to tell how helpful this technique could be for law enforcement. But with this and surreptitious DNA sampling it is likely that only the successes will be made public. Law enforcement officials are unlikely to publicize the failures, dead ends or number of people who are investigated without their consent or knowledge.

An over-reliance on these practices could well undermine law enforcement. Some law enforcement officials have expressed concern that the tremendous resources funneled into building and expanding forensic DNA banks are channeling money away that should be put into following up on investigational leads or placing police officers on the streets.[62] In addition, crime laboratories all over the country are plagued by extraordinary backlogs resulting from the heedless expansion of the databanks. In February, the California Commission on the Fair Administration of Justice, a bipartisan panel of criminal justice experts and practitioners, released an emergency report that documented enormous backlogs of about 160,000 untested DNA samples in California's state lab arising from the expansion of California's databank to all felons.[63] This backlog is expected to increase exponentially when Proposition 69's arrestee-testing provision comes into effect in 2009, when an additional 450,000 samples will be eligible for collection each year.

Backlogs can have tragic outcomes. As the California panel reported, "Delays of six months or more have become the norm" in analyzing rape kits in the state. In one case, a rapist attacked two more victims, including a child, while his DNA sat on a shelf awaiting analysis. Backlogs can also increase the chances of error in DNA analysis, labeling or interpretation as lab analysts are pressured to cut corners to meet their workload. Such errors have already resulted in a few known miscarriages of justice. Josiah Sutton spent nearly five years in prison, starting at the age of 16, for a rape he could not have committed as a result of an error made by an analyst at the Houston Crime Lab. In another case, a 26-year-old man faced life in jail and was incarcerated for over a year because the Las Vegas police crime lab mistakenly switched the label on his DNA sample with that of his cell mate.[64] Timothy Durham of Tulsa, Oklahoma spent four years in prison on the basis of a misinterpreted DNA test, despite having 11 alibi witnesses who placed him in another state at the time of the rape.[65]

---

[61] *See* Pam Belluck, *Slow DNA Trail Leads to Suspect in Cape Cod Case*, N.Y. TIMES, Apr. 16, 2005; *see also* Eileen McNamara, *Not Making his Case*, BOSTON GLOBE, Apr. 17, 2005.

[62] *See* Rockne Harmon, Assistant Dist. Att'y of Alameda County, Post-Conviction Review: A Prosecutor's Viewpoint, Remarks at the DNA Fingerprinting and Civil Liberties Workshop hosted by the American Society for Law, Medicine & Ethics (Sept. 2005).

[63] California Commission on the Fair Administration of Justice, Emergency Report and Recommendations Regarding DNA Testing Backlogs (Feb. 20, 2007).

[64] *See* Glenn Puit, *Man Files Lawsuit in False Imprisonment*, LAS VEGAS REV.-J. (2002).

[65] *See* W. C. Thompson, F. Taroni & C.G.G. Aitken, *How the probability of a false positive affects the value of DNA evidence*, J. OF FORENSIC SCI. (Jan. 2003).

The more that DNA is relied upon to create suspects where there are none, the more vulnerable it will be to abuse. Already, several instances have been reported where criminals have planted or tampered with DNA evidence, or paid inmates to take DNA tests as a way of confusing investigators or evading prosecution. Prisoners have also been overheard coaching each other on how to plant biological evidence at crime scenes and how to avoid leaving their own DNA behind. Just last week, four men in Massachusetts were indicted on charges of DNA tampering for allegedly attempting to switch identity bracelets while having blood drawn for a DNA sample while in custody.[66]

Finally, we will likely see increasing hostility among the public as law enforcement engages in DNA screens that impute suspicion based on neighborhood, vague physical descriptions or racial characteristics, or familial relations. Ultimately, people may be unwilling to cooperate with law enforcement in helping to resolve a crime where these practices become more routine and the rules as to whether and under what circumstances their DNA may be collected and used remain unclear.

VIII. Conclusion and Recommendations

We can hardly blame law enforcement for wanting to use DNA in any way possible to solve crimes. At the same time, privacy in one's DNA is completely undermined if law enforcement is permitted to use backdoor methods of DNA collection and examine DNA for any and all information about a person, including their personal characteristics and familial characteristics and connections.

Expansions of the uses of DNA by law enforcement are generally occurring in a policy vacuum and then being justified retroactively by a limited number of solved crimes aided by DNA data. Aside from the fact that these cases appear to be the exception rather than the rule, what is not revealed by these stories is the larger picture of the steady erosion of privacy that accompanies the shifting purpose of DNA's use by law enforcement from one of identification to surveillance. Continued use of these techniques and practices outside of the arena of judicial oversight and without the application of ethical guidelines should spark a rigorous debate about the government's intrusion into the lives of innocent people.

Once the information inscribed in DNA is considered private, then it follows that this principle should be embedded in the policy debate so that it can assist us in establishing an appropriate balance between law enforcement and civil liberties. That principle of balance should guide where and when DNA technology may be used by law enforcement. We offer the following basic recommendations as to how to achieve that balance:

1. Informed consent should be required before law enforcement takes or tests the DNA of a person who has not been convicted of a crime. Surreptitious taking, testing or storing of DNA from suspects or their relatives is a violation of a person's privacy and should be prohibited.

[66] *See* Buffy Spencer, *Four Men Charged with DNA Tampering*, THE REPUBLICAN, Mar. 17, 2007, at B02.

2. Absent valid consent, a court order based upon probable cause should be required for the taking of an individual's DNA. That DNA should be compared only with the DNA from a crime scene for which that person is a suspect.
3. DNA databanks should be limited to DNA profiles from persons who are convicted of serious crimes. All those presumed innocent do not have a diminished right to privacy and therefore should not have their DNA included in a forensic DNA databank.
4. Offender biological samples should be destroyed so that the encoded information cannot be mined for purposes beyond identification (such as investigating potential gene-behavior associations).
5. Crime scene samples should be analyzed only for purposes of identification. Law enforcement should generally be barred from looking for rare alleles that are associated with genetic diseases or other traits that are not central to identification.
6. The Genetic Nondiscrimination Act of 2007 should be passed and then amended to provide protections and rules for law enforcement. Otherwise, just as people have been hesitant to undergo genetic testing for fear that their information will be used against them by insurance companies or future employers,[67] so will they fear that law enforcement will mine their medical records for their DNA.
7. A court order based upon probable cause should be required for law enforcement to be given access to anyone's medical records for genetic data. The rules protecting medical information in HIPAA and their current broad exemption provided to law enforcement should be tightened to account for emerging interests in health data for forensic uses.

[67] *See Genetic Information Nondiscriminaton Act of 2007: Hearing on H.R. 493 Before the Subcomm. on Health of the H. Comm. on Energy and Commerce*, 110th Cong. (2007) (statement of the Honorable Francis S. Collins, Director, National Human Genome Research Institute).

Table 1.[68] STATE LAWS AUTHORIZING DNA RETENTION UPON ARREST

STATE	YEAR	ARRESTEES INCLUDED
TX (HB 588)	2001	Individuals indicted for certain sex crimes, certain crimes against children and burglary.
VA (HB 892)	2002	"Every person arrested for the commission or attempted commission of a violent felony"
LA (HB 66)	2003	"A person who is arrested for a felony or other specified offense, including an attempt, conspiracy, criminal solicitation, or accessory after the fact of such offenses." Other specified offenses include: battery, unlawful use of a laser on a police officer, simple assault, assault on a schoolteacher, stalking, misdemeanor carnal knowledge of a juvenile, prostitution, soliciting for prostitutes, prostitution by massage, letting premises for prostitution and peeping tom offenses. Includes juveniles.
CA (Prop. 69)	2004	Any adult person arrested for or charged with a felony sex offense or for murder or voluntary manslaughter or any attempt to commit those offenses; starting January 1, 2009 any adult person arrested for or charged with any felony offense.
MN[69]	2005	Arrests for violent felony or burglary, upon finding of probable cause for the arrest.
NM (SB 216)	2006	Requires DNA samples from all persons eighteen years of age or over who are arrested for certain felony offenses.
KS (HB 2554)	2006	Arrests for any felony or drug crime of severity levels 1 or 2.
TN (SB 1196)	2007	Any person arrested for a violent felony.
AK (HB 90)	2007	Anyone arrested for a violent felony or domestic abuse.
ND (HB 1197)	2007	Any adult arrested for a felony crime. Contingent upon federal funding being available to implement the act.
AZ (HB 2787)	2007	Any person arrested for a serious crime such as homicide, dangerous crimes against children and sexual offenses who is transferred by an arresting authority to a state, county or local law enforcement agency or jail.

[68] Table I prepared by T. Simoncelli with Joanne Kang, ACLU Washington Legislative Office.

[69] Declared unconstitutional. *See* In re Welfare of C.T.L., *supra* note 13 (declaring the statute unconstitutional, "because Minn.Stat. § 299C.105, subd. 1(a)(1) and (3) (2005), direct law enforcement personnel to conduct searches without first obtaining a search warrant based on a neutral and detached magistrate's determination that there is a fair probability that the search will produce contraband or evidence of a crime, and because the privacy interest of a person who has been charged with a criminal offense, but who has not been convicted, is not outweighed by the state's interest in taking a biological specimen from the person for the purpose of DNA analysis, the portions of Minn. Stat. § 299C.105, subd. 1(a)(1) and (3), that direct law-enforcement personnel to take a biological specimen from a person who has been charged but not convicted violate the Fourth Amendment to the United States Constitution and Article I, Section 10 of the Minnesota Constitution").