IN THE COURT OF APPEALS OF MARYLAND

September Term, 2003

No. 129

THE STATE OF MARYLAND,

Appellant,

v.

CHARLES RAINES,

Appellee.

On Writ of Certiorari to the Court of Special Appeals of Maryland

---

Brief of *Amicus Curiae* Electronic Privacy Information Center in Support of Appellee, Charles Raines, Urging Affirmance

---

MARC ROTENBERG
*CHRIS HOOFNAGLE
MARCIA HOFMANN
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue. NW, Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for *Amicus Curiae*

*Admitted in the State of Maryland

IN THE COURT OF APPEALS OF MARYLAND

STATE OF MARYLAND,	)	
	)	
Appellant,	)	Summer Term, 2003
	)	
v.	)	No. 129
	)	
CHARLES RAINES,	)	
	)	
Appellee.	)	
	)	

MOTION OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER FOR CONSENT TO FILE ACCOMPANYING *AMICUS* BRIEF

Pursuant to Maryland Rule 8-511, *amicus curiae* Electronic Privacy Information Center ("EPIC") requests consent to file the accompanying *amicus curiae* brief in support of Appellee Charles Raines. This brief urges affirmance of the Circuit Court for Montgomery County's decision. Both parties to this case have consented to the filing of this brief.

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has participated as *amicus curiae* in numerous privacy cases, including *Hiibel v. Sixth Judicial District Court of Nevada*, No. 03-5554 (2004), *Doe v. Chao*, 124 S. Ct. 1204 (2004), *Smith v. Doe*, 538 U.S. 84 (2003), *Dep't. of Justice v. City of Chicago*, 537 U.S. 1229 (2003), *Watchtower Bible and Tract Soc'y of N.Y. Inc. v. Vill. Of*

Stratton, 536 U.S. 150 (2002), *Reno v. Condon*, 528 U.S. 141 (2000), and *United States v. Kincade*, *reh'g granted*, No. 02-50380 (9th Cir. 2004).

In this case, the Maryland DNA Collection Act, Md. Code Ann., Pub. Safety, § 2-501 to § 2-512, compels the production of DNA samples in violation of the Fourth Amendment and Article 26 of the Constitution of Maryland. DNA reveals vastly more information than a fingerprint. DNA profiles may also implicate an individual's family. Moreover, the collection of DNA samples for inclusion in a state database that is part of a widely accessible national DNA database raises the very real possibility that DNA samples collected at one point in time for one purpose will be used in the future for unrelated purposes. EPIC believes it is vital to understand the extent to which DNA collection and use implicate Fourth Amendment and Article 26 interests, and therefore respectfully requests that this Court grant it consent to file the accompanying *amicus curiae* brief.

Dated: April 26, 2004

Respectfully submitted,

_____

MARC ROTENBERG
*CHRIS HOOFNAGLE
MARCIA HOFMANN
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for *Amicus Curiae*

*Admitted in the State of Maryland

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutory Authority

Other Authorities

FBI, U.S. Dep't of Justice, *Facts and Figures 2003, Law Enforcement Support* (last accessed April 26, 2004) 18

FBI, U.S. Dep't of Justice, *FBI CODIS – National DNA Index System* (March. 2004) . . .9

FBI, U.S. Dep't of Justice, *Protecting American Streets: Law Enforcement Information Sharing is Key* (Jan. 7, 2004) 18

FBI, U.S. Dep't of Justice, *Science and Technology in the Name of Justice, Part 2: FBI DNA Database Passes an Important Milestone* (Feb. 3, 2004) 9, 10

FBI, U.S. Dep't of Justice, *Standards for Forensic DNA Testing Labs* (last accessed April 26, 2004) 16

FBI, U.S. Dep't of Justice, *The FBI's Combined DNA Index System Program Brochure* (April 2000) 8, 9

G. Gardiner, DNA Profiling: Information Paper No 22/01 (2002) Victorian Parliamentary Library 15

General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Feb. 2004) 19

National Commission for the Future of DNA Evidence, National Institute of Justice, U.S. Dep't of Justice, *Future of Forensic DNA Testing: Predictions of the Research and Development Working Group*, NCJ 183697 (November 2000) . . . 7, 9, 13, 14, 16-17

National Institute of Justice, Office of Justice Programs, U.S. Dep't of Justice, *NIJ Special Report: Using DNA to Solve Cold Cases* (July 2002) 6, 7, 8, 11

Daniel J. Solove & Marc Rotenberg, *Information Privacy Law* (2003) 6

U.S. Dep't of Energy Office of Science et al., *DNA Forensics*, Human Genome Project Information (last modified Jan. 12, 2004) 2-3, 7, 11-12, 14

W. Austl. Police Serv., Sample Destruction (last accessed April 26, 2004). 15

STATEMENT OF *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established in 1994 to focus public attention on emerging civil liberties issues. EPIC has participated as *amicus curiae* in numerous privacy cases, including *Hiibel v. Sixth Judicial District Court of Nevada*, No. 03-5554 (2004), *Doe v. Chao*, 124 S. Ct. 1204 (2004), *Smith v. Doe*, 538 U.S. 84 (2003), *Dep't. of Justice v. City of Chicago*, 537 U.S. 1229 (2003), *Watchtower Bible and Tract Soc'y of N.Y. Inc. v. Vill. of Stratton*, 536 U.S. 150 (2002), *Reno v. Condon*, 528 U.S. 141 (2000), and *United States v. Kincade*, *reh'g granted*, No. 02-50380 (9th Cir. 2004).[1]

STATEMENT OF THE CASE

We adopt the statement of the case set forth in Appellee Charles Raines' brief before the Court of Appeals.

QUESTION PRESENTED

I. Does the compelled production of a DNA sample unrelated to a particular criminal investigation violate the Fourth Amendment and Article 26 of the Constitution of Maryland?

---

[1] EPIC Senior Fellow Anna Slomovic, Ph.D. and Policy Analysts Tiffany A. Stedman and Michael W. Trinh assisted in the preparation of this brief.

STATEMENT OF THE FACTS

We adopt the facts as set forth in Appellee Charles Raines' brief before the Court of Appeals.

SUMMARY OF ARGUMENT

Maryland courts generally construe Article 26 of the Constitution of Maryland *in pari materia* with the Fourth Amendment. However, Maryland law has also recognized the need in certain circumstances to provide more protection for privacy than federal statutes extend. For example, the Maryland Wiretapping and Electronic Surveillance Law, Md. Code Ann., Cts. & Jud. Proc. §§ 10-401 through 10-414 (2003), provides greater protection for telephone communications than the federal equivalent. The Court should take into account Maryland's well-established emphasis on protecting privacy as it examines the constitutionality of Maryland's DNA Act in this case.

The compelled production of a DNA sample unrelated to a particular criminal investigation violates the Fourth Amendment and Article 26. A DNA sample can provide intimate personal information, including:

> insights into many intimate aspects of a person and their families including susceptibility to particular diseases, legitimacy of birth, and perhaps predispositions to certain behaviors and sexual orientation. This increases the potential for genetic discrimination by government, insurers, employers, schools, banks, and others.

U.S. Dep't of Energy Office of Science et al., *DNA Forensics*, Human Genome Project Information (last modified Jan. 12, 2004).[2]

DNA reveals vastly more information than a fingerprint and therefore must be accorded strong Constitutional protection. DNA profiles may also implicate an individual's family. Moreover, DNA samples collected in Maryland are placed in a national DNA database. This database is already accessible to an international law enforcement agency and may soon interface with various government information systems that serve purposes other than law enforcement. Such expansion in the database's use raises the very real possibility that DNA samples collected in Maryland at one point in time for the purpose of criminal investigation will be used elsewhere in the future for purposes wholly unrelated to any law enforcement interest.

ARGUMENT

The compelled production of DNA samples unrelated to a particular criminal investigation pursuant to the Maryland DNA Collection Act, Md. Code Ann., Pub. Safety, § 2-501 to § 2-512 (the "DNA Act" or the "Act"), violates the Fourth Amendment and Article 26 of the Constitution of Maryland.

I. Maryland Law Favors Protection From Intrusions of Privacy

The State of Maryland has traditionally given great consideration to the impact of emerging technologies upon individual privacy. Though Maryland courts generally

---

[2] *At* http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml.

construe Article 26 *in pari materia* with the Fourth Amendment, *see Gadson v. Maryland*, 668 A.2d 22 (Md. 1995), and in accordance with the Supreme Court's interpretations of the Fourth Amendment, s*ee, e.g., Scott v. Maryland*, 782 A.2d 862 (Md. 2001); *Gahan v. Maryland*, 430 A.2d 49 (Md. 1981); *Givner v. Maryland*, 124 A.2d 764, 764 (Md. 1956), the Maryland General Assembly historically has crafted state law to give individuals greater protection from invasive searches than Federal law provides.

The Maryland General Assembly has traditionally afforded great deference to the privacy of an individual's physical person. For example, Maryland has regulated health care provider disclosures of medical records since 1990. Md. Code Ann., Health-Gen., § 4-305 (2003). Congress, however, did not comprehensively regulate the use and disclosure of health information until the passage of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 300gg et seq. (2003).

The Maryland General Assembly has also provided greater legal protections from intrusion than Federal law when emerging technologies are implicated. For instance, the Maryland Wiretapping and Electronic Surveillance Law, Md. Code Ann., Cts. & Jud. Proc. §§ 10-401 through 10-414 (2003), provides greater protection for the privacy interest in telephone communications than the Federal wiretap law, 18 U.S.C. § 2510 et seq. (2003), by requiring all parties to a conversation to consent to its recording. In *Mustafa v. Maryland*, the Maryland Court of Appeals explicitly characterized the purpose of the law as a means to protect privacy: "the two-party consent provision of the Maryland Act is aimed at providing greater protection for the privacy interest in communications than the federal law." 591 A.2d 481, 485 (Md. 1991). Later, in *Perry v.*

Maryland, the Court discussed the legislative history of the state wiretap law, explaining that:

> The requirement of consent by *all* parties for the recording of a telephone conversation by a private individual has been a fundamental part of Maryland law since at least 1956, and the one attempt by the Legislature, in 1973, to modify that provision met with a veto in which the Governor expressed his deep concern that the "opportunity for unwarranted spying and intrusions on people's privacy authorized by this bill is frightening."

741 A.2d 1162, 1175 (Md. 1999). (emphasis in original)

The Maryland General Assembly has not limited protection against electronic surveillance to that conducted via wiretap. Maryland law also criminalizes visual surveillance, including camera surveillance, conducted in private places without the consent of the observed. Md. Code Ann., Criminal Law, §§ 3-901 to 3-903 (2003). No equivalent protection currently exists under Federal law.

Even where State and Federal privacy laws involving technology are similar in scope, Maryland has historically provided privacy protections before Congress extended them nationally. For example, Maryland passed a law in 2002 prohibiting the transmission of deceptively labeled commercial e-mail. Md. Ann. Code, Commercial Law, § 14-3002 (2003). Federal law did not provide this protection to individuals until the passage in December 2003 of the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003, 15 U.S.C. 7701 et seq.

Because Maryland has historically taken more expedient and greater measures than the Federal government to protect individuals against invasions of privacy related to technology, this Court should consider very carefully the importance of protecting

individuals from the intrusions inherent in DNA collection and use under Maryland's DNA Act. Supreme Court Justice Louis Brandeis once noted, "It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country." *New State Ice Co. v. Lieberman*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting). We urge this Court to follow this approach, as Maryland has before when advances in technology presented threats to the privacy of the individual, and extend greater Constitutional protections to those who are compelled to provide DNA samples under the DNA Act.

II. Overview of the Combined DNA Index System ("CODIS")

There is an effort underway to expand DNA collection to all arrestees in the United States. Daniel J. Solove & Marc Rotenberg, *Information Privacy Law* 268 (2003). This collected DNA is gathered in a FBI-maintained national DNA database known as the Combined DNA Indexing System ("CODIS"). The FBI Laboratory's CODIS program allows federal, state, and local crime laboratories to collect, exchange and compare DNA profiles electronically. National Institute of Justice, Office of Justice Programs, U.S. Dep't of Justice, *NIJ Special Report: Using DNA to Solve Cold Cases* 9 (July 2002) [hereinafter *Using DNA to Solve Cold Cases*].[3] The FBI has selected short tandem repeat ("STR") technology to generate profiles for CODIS from collected DNA. *Id.* at 6. STR technology is used to evaluate 13 specific regions, known as loci or

[3] *At* http://www.ncjrs.org/pdffiles1/nij/194197.pdf.

markers, within DNA located in a cell's nucleus. U.S. Dep't of Energy Office of Science et al., *DNA Forensics*, Human Genome Project Information (last modified Jan. 12, 2004) [hereinafter *DNA Forensics*].[4] The 13 STR loci are located within "junk DNA," or DNA with no currently known function. National Commission for the Future of DNA Evidence, National Institute of Justice, U.S. Dep't of Justice, *Future of Forensic DNA Testing: Predictions of the Research and Development Working Group*, NCJ 183697 12 (November 2000) [hereinafter *Future of Forensic DNA Testing*].[5] The National Commission on the Future of DNA Evidence has stated that the 13 STR loci used to generate a CODIS profile "are not associated with specific, observable traits." *Id*. at 35. However, an individual's sex can already be determined from the 13 STR loci. *Id.* at 60. Furthermore, it is possible to calculate the likelihood that an individual belongs to a certain race from the 13 STR loci. *Id*. at 35.

CODIS consists of three hierarchical tiers—local, state, and national—which operate in tandem as a nationally distributed database. *Using DNA to Solve Cold Cases, supra,* at 10. The National DNA Index System ("NDIS") is the highest tier, and makes it possible for all laboratories participating in CODIS to access and compare DNA profiles from across the country. *Id*. The second tier is the State DNA Index System ("SDIS"). *Using DNA to Solve Cold Cases, supra,* at 10; s*ee, e.g.,* Md. Code Ann., Pub. Safety, § 2-502 (2003) (establishing "statewide DNA database" in the Maryland Crime Laboratory). The third tier is the Local DNA Index System ("LDIS"), where DNA profiles are entered

---

[4] *At* http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml.
[5] *At* http://www.ncjrs.org/pdffiles1/nij/183697.pdf.

into the system by participating forensic labs throughout the country. *Using DNA to Solve Cold Cases, supra,* at 10. The tiered nature of the system enables each state and local agency to operate its DNA database and gather DNA samples in compliance with state and local laws. *Id*.; s*ee, e.g.,* Md. Code Ann., Pub. Safety, § 2-504 (2003).

DNA profiles in CODIS are organized in two indices: the Forensic Index and the Offender Index. FBI, U.S. Dep't of Justice, *The FBI's Combined DNA Index System Program Brochure* (April 2000).[6] The Forensic Index contains DNA profiles culled from crime scene evidence. *Id*. The Offender Index contains DNA profiles of individuals collected under applicable federal, state, or local laws. *Id*. The Offender Index is where profiles collected from individuals under the various state DNA Acts are maintained.

CODIS matches DNA profiles to those in the Forensic Index to link crime scenes together, indicating the possibility of serial crimes. *Id*. Matches may also be made between profiles stored in the Offender Index and the Forensic Index to potentially link an individual's DNA profile to DNA found at a crime scene, tentatively identifying the perpetrator of the crime. *Id*. When such a match occurs, DNA analysts at the labs responsible for entering the matching profiles work together to confirm or invalidate the match. *Id*.

The stated purpose of CODIS is to identify those present at the scene of a crime. There are separate databases for victim DNA and perpetrator DNA. In 2000, the National Institute of Justice advised that in the future, DNA databanks would vastly

---

[6] *At* http://www.fbi.gov/hq/lab/codis/brochures.htm.

expand to include DNA from the general public, further encroaching upon personal privacy:

> Inevitably, there will be the increasing possibility of broadening the database to include the general public. There would be many advantages, such as identification of persons or body parts after accidents, or discover of kidnapped or lost people. At the same time, the risk to individual privacy would be enhanced and protection of anonymity would be harder.

Future of Forensic DNA Testing, supra, at 35-36.

As of March 2004, CODIS contained 1,719,551 DNA profiles. FBI, U.S. Dep't of Justice, *FBI CODIS – National DNA Index System* (March 2004) [hereinafter *CODIS –National DNA Index System*].[7] The number of profiles has grown rapidly from 210,000 profiles in April 2000. FBI, U.S. Dep't of Justice, *Combined DNA Index System Programs* (April 2000).[8] Of the nearly 1.7 million DNA profiles, 1,651,076 profiles are of convicted persons, and the remaining 78,745 DNA profiles are created from DNA evidence gathered from crime scenes, missing persons, relatives of missing persons, and unidentified remains. *CODIS—National DNA Index System; see* FBI, U.S. Dep't of Justice, *Science and Technology in the Name of Justice, Part 2: FBI DNA Database Passes an Important Milestone* (Feb. 3, 2004) [hereinafter *FBI DNA Database Passes an Important Milestone*].[9] CODIS connects the 175 crime labs and the DNA databases of 48 states, the U.S. Army, the FBI, and Puerto Rico. FBI, U.S. Dep't of Justice, *CODIS*

---

[7] *At* http://www.fbi.gov/hq/lab/codis/national.htm.
[8] *At* http://www.fbi.gov/hq/lab/codis/brochure.pdf.
[9] *At* http://www.fbi.gov/page2/feb04/codis020304.htm.

Participating States (Jan. 2004) (only Mississippi and Rhode Island do not participate in CODIS);[10] *FBI DNA Database Passes an Important Milestone*, *supra.*

III. DNA Contains Substantially More Information than a Fingerprint

The State of Maryland contends that the collection of a DNA sample is equivalent to the collection of a fingerprint, since both provide a positive means of identification. (App. Br. at 1-2.) However, information from a DNA sample reveals far more personal information than the mere identification available from a fingerprint. Because this information in human DNA provides extensive personal information not relevant to identification, the compelled collection of DNA information absent individualized suspicion for a particular crime constitutes a form of general search and thus violates the Fourth Amendment and Article 26. If the state purpose for the DNA collection is solely identification, the collection provides much more information than is needed for that narrow purpose. DNA collection for identification, therefore, constitutes an impermissible extension of the narrow authority to search.

If the state purpose for DNA collection is broader than identification, then the information is collected for general crime control purposes, which is squarely controlled by *Indianapolis v. Edmond*, 531 U.S. 32 (2000). *Edmond* clearly prohibits such collection when its purpose is indistinguishable from general law enforcement purposes. *Id*. at 47-48. In either case, the compelled collection of DNA violates the Fourth

---

[10] *At* http://www.fbi.gov/hq/lab/codis/partstates.htm.

Amendment and Article 26 because of the extensive amount of individual personal information collected in a compelled DNA sample.

As this Court ruled in *Gadson v. Maryland*, police action is limited to the purpose of a search by the Fourth Amendment unless there is "reasonable, articulable suspicion" that justifies further investigation. 668 A.2d 22 (Md. 1995). As discussed below, a DNA sample is a rich source of highly personal information that is useful for reasons other than mere identification. This specific and detailed information is only relevant to a legitimate law enforcement use in the context of a pending criminal investigation. Otherwise, the compelled collection of this individual information is useful only for general crime control purposes, or for non-public safety-related purposes, which is clearly unconstitutional.

Law enforcement use of DNA profiles bears only superficial similarity to law enforcement use of fingerprints. Both a fingerprint and DNA profile are compared to evidence collected from a crime scene to determine whether there are matching identifying features. *Using DNA to Solve Cold Cases, supra*, at 5. However, the information obtained from a DNA sample is far more extensive. According to the Human Genome Project, coordinated by the Department of Energy and National Institutes of Health to map and study the entire human genetic sequence:

> DNA profiles are different from fingerprints, which are useful only for identification. DNA can provide insights into many intimate aspects of a person and their families including susceptibility to particular diseases, legitimacy of birth, and perhaps predispositions to certain behaviors and sexual orientation. This increases the potential for genetic discrimination by government, insurers, employers, schools, banks, and others.

DNA Forensics, *supra.*

The information obtained from a DNA sample extends beyond simple identification of a person because DNA sampling uses information that defines many aspects of an individual. According to the Human Genome Project: "there is a chance that a person's entire genome may be available — criminal or otherwise. Although the DNA used is considered 'junk DNA' . . . in the future this information may be found to reveal personal information such as susceptibilities to disease and certain behaviors." *Id*.

The report of a major, two-year inquiry by the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council likewise found a substantial distinction between a DNA profile and fingerprint:

> Media and other accounts often suggest that DNA profiles are simply a modern form of fingerprint identification. In fact, DNA profiles differ from conventional fingerprints in several important respects. First, DNA holds vastly more information than fingerprints. A DNA profile can be used in establishing kinship relationships, and the sample from which the profile was obtained may hold predictive health and other information of a sensitive nature. Second, as genetic information is shared with biological relatives, an individual's profile might indirectly implicate a relative in an offence. Third, while it can be difficult to obtain fingerprints of such quality as to be useful in an investigation, DNA can be amplified from tiny and aged samples, and may be recovered from almost any cell or tissue.

Essentially Yours: The Protection of Human Genetic Information in Australia (2003).[11]

DNA profiles may also implicate an individual's family. "With 13 STR loci it is quite likely that a search of a database will identify a person who is a relative of the

---

[11] *Available at* http://www.austlii.edu.au/au/other/alrc/publications/reports/96/.

person contributing the evidence sample." *Future of Forensic DNA Testing, supra,* at 35. Profile matches occur between individuals with sibling and parent-children relationships. *Id*. Other close familial relationships can result in a profile match, though with less certainty. *Id*. Such matches can result in situations in which individuals may be investigated by law enforcement merely for having a relative whose DNA was collected at a crime scene. This problem is likely to encourage the expansion of DNA profiles to include additional markers: "In addition to database development, a variety of genetic markers will find special applications in cases requiring information on family lineage, difficult samples, and investigative problems." *Id*. at 34.

Because significant resources have been invested in CODIS, it is likely that the 13 STR loci on which CODIS profiles are based will continue to be used well into the future, along with possible additions of other markers. *Id.* at 20. Therefore, future DNA collection could be even more invasive and provide more information unrelated to identification to the government.

IV. DNA Samples Can be Reanalyzed for Non-Law Enforcement Purposes

Because of the detailed nature of the information contained, DNA samples can be used for purposes unrelated to identification. There is a significant possibility that the samples will be sought by others for purposes unrelated to those purposes of the initial collection. In 2000, a working group of the National Institute of Justice submitted a report that outlined some of the group's concerns about DNA collection, storage, and analysis. *See Future of Forensic DNA Testing, supra*. In this report, the authors

cautioned that although "the majority of States now have sample storage policies," "[a]t present, there is no clear overall policy as to what happens to the DNA sample after profiles are added to the database." *Id.* at 36. In reality, "[c]ollected samples are stored, and many state laws do not require the destruction of a DNA record or sample after a conviction has been overturned." *DNA Forensics, supra.*

According to the National Institute of Justice report:

> It can be argued that saving the DNA permits retesting and inclusion of additional loci, particularly newly discovered ones. This would be much more efficient than searching out the person, who may not even be living. On the other side, it is argued that the profiles are recorded and that this information is all that is needed, not the DNA itself. Furthermore, those fearful of invasion of privacy are concerned lest the DNA become available to unauthorized parties or otherwise be used in ways that would disclose information that ought to remain confidential.

Future of Forensic DNA Testing, *supra*, at 36.

Over a decade ago, the National Academy of Sciences recommended that samples be destroyed "promptly" after analysis. Comm. on DNA Tech. in Forensic Science of the Nat'l Acad. of Science, *DNA Technology in Forensic Science* 122 (Nat'l Acad. Press 1992). Stated the Academy: "In principle, retention of DNA samples creates an opportunity for misuses—i.e., for later testing to determine personal information. In general, the committee discourages the retention of DNA samples." *Id.* The Academy stressed that "investigation of DNA samples or stored information for the purpose of obtaining medical information or discerning other traits should be prohibited, and violations should be punishable by law." *Id.* at 116.

Privacy concerns have led several countries to take steps to reduce the risk of subsequent misuse of DNA samples.[12] For example, under Australian law, crime victims, witnesses to a crime, and anyone who volunteers DNA for police use may limit the use of their DNA for certain purposes and request that it be destroyed. W. Austl. Police Serv., *Sample Destruction* (last accessed April 26, 2004).[13] A crime suspect may also request destruction of his sample after a not guilty verdict or within two years of its acquisition if no charge is brought. *Id*. A requester need only make his request in writing to the designated person in charge of request. *Id*. New Zealand, Germany, Sweden, Denmark and the Netherlands currently require samples to be destroyed after the profile has been created. G. Gardiner, *DNA Profiling: Information Paper No 22/01* (2002) Victorian Parliamentary Library 16. As one expert panel recently concluded:

> The Inquiry confirms its preliminary view that the balance should be tipped in favour of physical destruction of forensic material and information obtained from it, in order to maintain information security and public confidence in the use of DNA profiling for criminal investigations. However, in relation to profiles, where there is no capacity for further testing, it would be sufficient protection for these to be permanently and irreversibly de-identified. It should be noted in this context that coded data should not be considered 'de-identified' because coding, by its very nature, is reversible.

---

[12] Legal protection for DNA samples varies widely around the world. *See generally* Electronic Privacy Information Center, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (2003) [hereinafter *Privacy and Human Rights*].

[13] *Available at* http://www.police.wa.gov.au/AboutUs/AboutUs.asp?DestructionDNA.

Australian National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* [15.8], [16.13], NHMRC, Canberra (1999).[14]

In contrast, the Department of Justice is seeking to impose broad retention requirements absent federal authority. The FBI quality assurance standards for labs participating in CODIS state: "Where possible, the laboratory shall retain or return a portion of the evidence sample or extract." *See* FBI, U.S. Dep't of Justice, *Standards for Forensic DNA Testing Labs* (last accessed April 26, 2004).[15] Thereby, specimens may be stored indefinitely in case a profile is challenged or testing technology improves. The Maryland DNA Act follows this approach by indefinitely maintaining DNA samples after profiling. Md. Code Ann., Public Safety § 2-506(b) (2003).[16]

DNA samples that are retained by laboratories or law enforcement could be reanalyzed in the future to gather more information than the profile now contains, as it becomes possible to identify new markers.

> [T]he loci now used for forensic identification and likely to be used in the future are not individually indicative of any external appearance. But a search for markers associated with specific traits will ultimately reveal them. Some laboratories are actively searching for such marker genes. For example, determining that a DNA sample was left by a person with red hair, dark skin pigment, straight hair baldness, or color blindness may be practical soon, if not already.

---

[14] *At* http://www.austlii.edu.au/au/other/alrc/publications/reports/96/41_Criminal_Investigations.doc.rtf.

[15] *At* http://www.fbi.gov/hq/lab/codis/forensic.htm.

[16] ("each DNA sample shall be stored securely and maintained by the Crime Laboratory in the statewide DNA repository").

Future of Forensic DNA Testing, supra, at 61. "Genetic markers for eye, hair, and skin color, for color-blindness, for baldness, and for less common traits such as albinism will soon be discovered, if they have not been already. We can expect the number [of identified genetic markers] to increase rapidly." *Id.* at 35.

Creating large DNA databases for the purposes of criminal investigation, such as CODIS, invites the danger of misuse of the DNA data for non-criminal investigation. It is also conceivable that soon, if not already, scientists will request access to what would serve as preexisting goldmine of DNA data for their research. With access to such information, the scientists will argue the potential benefit to humanity in studying gene patterns among those persons with a propensity for criminal activity. The National Institute of Justice clearly foresaw situation:

> As [CODIS] enlarges and if it is broadened to include persons convicted of a larger variety of crimes, it might be possible that statistical studies of the databases could reveal useful information. Inventive researchers may glean useful information of as statistical sort. At the same time, there would need to be protection against misuse or use by unauthorized persons.

Future of Forensic DNA Testing, supra, at 36. Surely this is the precise type of research encompassed by the executive administration's sweeping goal of "maximiz[ing] the use of the forensic sciences in the criminal justice system." *Advancing Justice through the Use of DNA Technology*, Statement of the White House (March 2003).[17]

---

[17] *Available at* http://www.whitehouse.gov/infocus/justice/dna_initiative-crime.html. The statement has been followed by legislation in Congress that would greatly expand the size and scope of CODIS. *See* H.R. 3214, 108th Cong. (2003).

V. National and International Governmental Entities May Soon Obtain Unregulated Access to an Individual's DNA Profile in CODIS

Currently, CODIS information is referenced within the National Criminal Information Center (NCIC), another database used for law enforcement purposes. Criminal Justice Info. Servs. (CJIS) Div. of the FBI, *National Crime Information Center (NCIC) Technical and Operational Update (TOU) 03-3*, at 2-5 (July 28, 2003) [hereinafter *NCIC Technical and Operational Update*].[18] The NCIC is the most extensive system of criminal history records in the United States, containing information on more than 52 million individuals and averaging 3.5 million transactions a day. FBI, U.S. Dep't of Justice, *Protecting American Streets: Law Enforcement Information Sharing is Key* (Jan. 7, 2004); [19] FBI, U.S. Dep't of Justice, *Facts and Figures 2003, Law Enforcement Support* (last accessed April 26, 2004).[20]

Each individual's profile in the NCIC documents the availability of a DNA sample, and lists the individual's CODIS file number, if existent. *NCIC Technical and Operational Update, supra*, at 2-5. At least one Bureau aspires to integrate the NCIC, CODIS, and other various searchable systems. *See* Bureau of Immigration & Customs Enforcement of the Dep't of Homeland Sec., *Endgame: Office of Detention & Removal Strategic Plan*, 2003-2012, at 4-8 (Aug. 15, 2003).[21]

The NCIC also interfaces with the United States Visitor and Immigrant Status

---

[18] *Available at* http://acjic.state.al.us/documents/TOU/tou03-3.pdf.
[19] *Available at* http://www.fbi.gov/page2/jan04/cjis010704.htm.
[20] *Available at* http://www.fbi.gov/libref/factsfigure/lawenforce.htm.
[21] *At* http://www.ice.gov/graphics/about/organization/endgame.pdf.

Technology (US-VISIT) and may soon interface with the second generation Computer Assisted Passenger Prescreening System. Dep't of Homeland Sec., *US-VISIT Program, Increment 1, Privacy Impact Assessment* at n.2 (Dec. 18, 2003)[22] [hereinafter *Privacy Impact Assessment*]; General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 at 29 (Feb. 2004).[23] US-VISIT, recently launched at 115 airports and 15 seaports, uses information from the NCIC and other sources to determine whether visitors traveling to the United States will be permitted into the country. *Privacy Impact Assessment* at 1. US-VISIT is accessible to Department of Homeland Security and Department of State employees, as well as local, state, and federal law enforcement. *Id*. at 5.

Further, CODIS is available to international law enforcement, including Interpol. *Diplomacy and the War on Terrorism: Hearing Before the Comm. on Foreign Relations, United States Senate*, 108th Cong. 2 (Mar. 18, 2003) (statement of John S. Pistole, Deputy Assistant Dir., Counterterrorism Div., FBI) ("The FBI Laboratory also has been engaged . . . to ensure that numerous international law enforcement partners are aware of the availability of the FBI's [CODIS] for assisting in the identification through DNA data of terrorists subjects and other criminal suspects.").[24] At present, there are no legal safeguards that prevent the possible misuse of information contained in CODIS by foreign law enforcement agencies. Further, there is no baseline federal protection for the

---

[22] *Available at* http://www.epic.org/privacy/us-visit/us-visit_pia.pdf.
[23] *Available at* http://www.epic.org/privacy/airtravel/gao-capps-rpt.pdf.
[24] *Available at* http://foreign.senate.gov/testimony/2003/PistoleTestimony030318.pdf.

DNA databases that forbid the use of samples for other purposes. Moreover, the government has already shown its willingness to share the information internationally and release the data into the hands of other nations, whose future use, either legally or scientifically, cannot be confined. *Id*. This problem is likely to increase dramatically with the growth in the number of characteristics that can be gleaned from DNA samples, along with the predicted expansion of the DNA databanks. Without constitutional limitations on the collection of DNA samples, the potential for abuse is great.

CONCLUSION

The broad compelled production of DNA samples pursuant to the Maryland DNA Collection Act, Md. Code Ann., Pub. Safety § 2-501 to § 2-512, violates the Fourth Amendment and Article 26 of the Constitution of Maryland. For the reasons set out above, the decision of the Circuit Court for Montgomery County should be affirmed.

Respectfully submitted,

_____

MARC ROTENBERG
*CHRIS HOOFNAGLE
MARCIA HOFMANN
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for *Amicus Curiae*

*Admitted in the State of Maryland

New Times Roman 13 Point

CERTIFICATE OF SERVICE

I hereby certify that on this 26th day of April, 2004, two copies of the forgoing *amicus curiae* brief were served on the following by First Class U.S. mail:

Stephen B. Mercer, Esq.
Sandler & Mercer, P.C.
27 West Jefferson Street
Suite 201
Rockville, MD 20850

Gary E. Bair
Solicitor General
Office of the Attorney General
Criminal Appeals Division
200 Saint Paul Place
Baltimore, MD 21202

_____
Chris Hoofnagle