HEALTH LAW, ETHICS, AND HUMAN RIGHTS

Protecting Privacy and the Public — Limits on Police Use of Bioidentifiers in Europe

George J. Annas, J.D., M.P.H.

Since 9/11, police and military around the world have sought to increase their arsenals of bioidentifiers, and privacy advocates have sought to cabin their use. In what may turn out to be the most important court decision involving the privacy limits on police use of bioidentifiers by any court in the world to date, the European Court of Human Rights ruled late last year that the United Kingdom's laws governing the collection and retention of DNA profiles and samples by law enforcement officials violate the human rights of members of the Council of Europe.[1] The Council of Europe, founded by 10 countries in 1949, currently has 47 member countries. The Council adopted the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1950, and it is the core document of the most comprehensive regional system of human rights protection in the world. Remarkably, the opinion was unanimous — signed by all 17 judges who were sitting as a Grand Chamber of the Human Rights Court — holding that the United Kingdom's retention policy "constitutes a disproportionate interference with the . . . right to respect for private life and cannot be regarded as necessary in a democratic society."[1]

The United Kingdom has been the world leader in collecting and using DNA profiles for criminal investigations since its first DNA dragnet, recounted vividly in Joseph Wambaugh's 1989 book, *The Blooding*. The book recounts how application of Alec Jeffreys's then-new DNA profiling technique was used to conduct a DNA dragnet that involved the collection of blood samples from more than 5000 men who lived in the vicinity of the location where two teenage girls had been brutally raped and murdered in 1983 and 1986.[2] Use of DNA profiling by the police was initially justified for identifying rapists and child molesters but has gradually expanded to involve more and more criminal suspects, although its usefulness in improving crime detection remains contested.[3] The expansion of bioidentification databases has also been justified by the threat of terrorism.[4] Because of the pioneering work in this area in the United Kingdom, the rules it adopts and the procedures it follows have considerable influence, especially in the United States, where our trend is to collect and retain DNA samples from all persons arrested for felonies.[5]

The constitutionality of the police's taking and using biometric data for identification and investigation, including not just DNA profiles but also fingerprints themselves, has never been examined by the U.S. Supreme Court. One recurring question is whether DNA information is in some way unique, such that it calls for special legislation and regulation, or whether our privacy laws that protect private information (including medical information) are sufficient. In addition, whether Europe takes privacy more seriously than America is open to debate.[6] Finally, whether the European opinion will influence judicial decisions in the United States depends on both the respect U.S. judges accord to non-U.S. judicial opinions and differences in the language of the European Convention and the U.S. Constitution.

S. AND MARPER IN THE UNITED KINGDOM

S. was arrested and charged with attempted robbery when he was 11 years of age; he was later acquitted. Michael Marper, an adult, was arrested and charged with harassment of his partner. Marper and his partner were reconciled before a pretrial review, and the case was formally discontinued. Both arrests occurred in 2001. In each case, the police took both fingerprints and DNA samples.

S. and Marper asked that their fingerprints and DNA samples be destroyed, and in both cases the police refused. An administrative court refused to reverse this decision, and it was upheld in a Court of Appeal decision on a two-to-one vote.

One of the judges in the majority, Lord Justice Waller, argued that although the actual DNA sample had major differences from the DNA profiles and fingerprints, retention of the samples themselves could be justified for five reasons that outweighed any risk to privacy[7]:

> Retention of samples permits (a) the checking of the integrity and future utility of the DNA database system; (b) a reanalysis for the upgrading of DNA profiles where new technology can improve the discriminating power of the DNA matching process; (c) reanalysis and thus an ability to extract other DNA markers and thus offer benefits in terms of speed, sensitivity and cost of searches of the database; (d) further analysis in investigations of alleged miscarriages of justice; and (e) further analysis so as to be able to identify any analytical or process errors.

An appeal to the House of Lords was dismissed, with Lord Steyn giving the lead judgment. He argued, among other things, that the reason U.K. law permitted the retention of DNA profiles and samples was to prevent cases in which persons who had been acquitted of rape or murder nonetheless later commit these crimes and escape prosecution because their samples had not been retained. He also relied on evidence that suggested that almost 6000 DNA profiles that had been linked with crime-scene stain profiles involving 53 murders and 94 rapes would have been destroyed under the rules requiring destruction after acquittal.

Lord Steyn concluded that any interference with private life was proportionate to what was necessary for investigation of the crime: that profiles and samples were kept only for the limited purpose of detection, investigation, and prosecution of crime; were not made public; and were not identifiable by a nonexpert. He also did not believe that retention of a sample in any way stigmatized the person whose sample was retained by treating them as a suspect in future crimes or that there was any difference between retaining a DNA profile and retaining a DNA sample.[1]

S. AND MARPER IN THE EUROPEAN COURT OF HUMAN RIGHTS

S. and Marper thereafter brought a complaint to the European Court of Human Rights, arguing that the actions of the United Kingdom in retaining their fingerprints, DNA profile, and DNA samples for purposes of criminal investigation violated their rights under Article 8 (right to respect for private and family life) of the European Convention which provides that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The court found that at least 20 of the 47 member states in the Council of Europe permit the compulsory taking of DNA information and its storage in national databases. Of these 20 members, the United Kingdom is the only one "expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued," and also is the only one "expressly to allow the systematic and indefinite retention of both profiles and samples of convicted persons."[1]

S. and Marper argued that retention of their DNA samples, DNA profiles, and fingerprints interfered with their right to respect for private life because this personal information is linked to personal identity and is the type of information they were entitled to keep within their control. DNA samples were of particular concern because they "contained full genetic information about a person including genetic information about his

or her relatives." The government agreed that all three were "personal data" but disagreed that any fell within the provisions of Article 8 of the European Convention because, unlike the actual taking of the information, the retention of it "did not interfere with the physical and psychological integrity of the person, nor did it breach their right to personal development or to establish and develop relationships with other human beings."[1]

THE HUMAN RIGHTS COURT DECISION

The court began its assessment by noting that the concept of "private life" is a broad one, covering not only the physical and psychological integrity of a person but also gender identification, name and sexual orientation, health information, ethnic identity, and other elements "relating to a person's right to their image." Most important, "the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8."[1] The court reviewed the retention of DNA samples, DNA profiles, and fingerprints separately.

Regarding DNA samples, the primary concern of S. and Marper was that the samples could be used in the future in new and currently unknown ways. The court agreed that such a concern, although speculative and not yet realized, "is legitimate and relevant to a determination of the issue of whether there has been an interference." The court continued:

> [samples] contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives. . . . Given the nature and amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned.[1]

Next is the DNA profile, which the United Kingdom argued was "nothing more than a sequence of numbers or a bar-code containing information of a purely objective and irrefutable character." The court had little sympathy for this argument, noting that although the information itself may be considered objective, the way it is used undercuts this description. In particular, the court noted that the profiles have been used for "familial searching with a view to identifying a possible genetic relationship between individuals" and that this use alone "is sufficient to conclude that their retention interferes with the right to the private life of the individual concerned." In addition, the court noted that police also use DNA profiles to assess the probable ethnic origin of a perpetrator, "which makes retention all the more sensitive and susceptible of affecting the right to private life."

Fingerprints obviously do not contain the type of personal, familial, ethnic, and health information contained in DNA. In previous cases, the court had concluded that retention of fingerprints and their closest analogue, photographs, by the police after an arrest did not present a privacy problem because they did not contain any subjective information that "called for refutation." For example, the court had previously found that retention of photographs taken at a demonstration did not interfere with private life, at least if authorities had not tried to identify the persons photographed by comparing the photograph with others in a data bank. On the other hand, the court found that retention of the recording of a person's voice did amount to interference with the right to respect for private life if it was used to try to identify the person "in conjunction with other personal data." Applying these cases to fingerprints, the court found that although fingerprints are neutral, objective, and unintelligible to the untutored eye, fingerprints nonetheless "contain unique information about the individual concerned[,] allowing his or her identification with precision in a wide range of circumstances." Because of this, they are capable of affecting private life, and therefore their blanket and indefinite retention "without the consent of the individual concerned cannot be regarded as neutral or insignificant."[1]

JUSTIFICATION FOR RETENTION IN A DEMOCRACY

The only remaining issue was whether the United Kingdom had a sufficient justification for retaining the DNA samples, DNA profiles, and fingerprints under Article 8 of the European Convention. S. and Marper argued that the justification of prevention or detection of crime was too vague and open to abuse and that indefinite retention could not be regarded as necessary in a demo-

cratic society for the purpose of preventing crime and was, in any event, disproportionate and particularly detrimental to children and members of certain ethnic groups overrepresented in the database.

The United Kingdom defended its indefinite retention as being of "inestimable value in the fight against crime and terrorism and the detection of the guilty" and the elimination of the innocent from suspicion. The United Kingdom also cited examples of successful prosecutions involving the retention of samples from people who had not been convicted, and it argued that the retention could not be regarded as excessive because the DNA samples and the DNA profiles were kept only for specific limited statutory purposes and were stored securely. In the government's view, there was no stigmatization and "no practical consequences for the applicants unless the records matched a crime-scene profile."[1]

The court found that the justification of preventing crime was so general that it could "give rise to extensive interpretation," saying:

> It is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[1]

The court agreed that prevention and detection of crime, particularly organized crime and terrorism, are both legitimate and increasingly reliant on modern scientific techniques, including DNA analysis. Nonetheless, the court was concerned that in the United Kingdom no distinctions are made on the basis of the gravity of the offense charged or the age of the suspect, and there are no time limits on retention, few opportunities to have the material destroyed, and no opportunity for independent review if a request for destruction is denied.

The court found especially troubling the risk of stigmatization from indefinite storage, which it believed undercut the presumption of innocence to which people who had not been convicted of any crime are entitled. Instead, these innocents were treated exactly the same as convicted criminals. This is even worse in the case of minors and members of ethnic minorities, who are overrepresented in the database. The court also found the retention of DNA samples to be "particularly intrusive given the wealth of genetic and health information contained therein."[1]

The court's ultimate conclusion, nonetheless, made no distinctions among DNA samples, DNA profiles, and fingerprints because of the "blanket and indiscriminate nature of the powers of retention" and the failure of the United Kingdom to strike a "fair balance between the competing public and private interests." The court accordingly held that blanket and indefinite retention of all three identifiers constituted a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. Therefore, the practice was in violation of Article 8 of the European Convention.[1]

IMPLICATIONS OF THE DECISION

The numbers are impressive. With more than 5 million DNA profiles and samples (representing 9% of the population, nearly all men), the United Kingdom's criminal DNA database is one of the largest in the world.[8] Of the 5 million, almost 1 million are from persons who were never convicted of any crime, and about half a million are from juveniles. The response to the European Court's decision in the United Kingdom has been largely positive. The journal *Nature,* for example, editorialized that although "technology can be a powerful force for human rights," it could also lead us down the road to a "surveillance society."[9]

The editors were particularly concerned that "without strong safeguards [legitimate databases] . . . could slowly and steadily be linked into an all-pervasive monitoring system that would make George Orwell's concept of 1984 look technologically tame all in the name of security, efficiency and convenience."[9] Alec Jeffreys himself also agreed with the decision, telling the *Guardian* newspaper that DNA samples should not be kept and that the DNA profiles of innocent people should not be in the data bank.[10] The U.K. government itself has issued a responsive set of proposals (out for public comment until August 7) to reform its practices.[11] The major proposal is

to end the practice of retaining DNA samples at all and to destroy them soon after the DNA profile is created.[11] As for the DNA profiles, as well as fingerprints, these would be retained for 6 years for those not convicted and for 12 years for those not convicted but charged with serious violent, sexual, or terrorism-related offenses.[11] There would be separate but similar rules for minors. The proposal to destroy all DNA samples is stunning, goes well beyond the ruling, and is to be applauded. The 6- and 12-year retention times, on the other hand, seem excessive, and they may be reduced further depending on public reaction.

The Marper opinion should also serve as an opportunity to reevaluate biometric identification policies in the United States. Fingerprinting, for example, has long been limited to arrestees and some federal employees, leaving other Americans alone, although since 9/11 there have been many additional instances of fingerprinting, including fingerprinting of visitors to the Statue of Liberty. New U.S. regulations also permit the storing of DNA data from arrestees from the states that collect their DNA and from all noncitizens detained by authorities for any purpose even if no charge is made or conviction obtained.[12]

It has been observed that all three identifiers in the United States "reflect arrest patterns, policing patterns, policing practices, and biases in judicial outcomes and as such are likely to reflect race, class, and geographic inequities."[13,14] Nonetheless, once entered in a data bank, they take on the appearance of objective, even scientific, data. Perhaps this is why their use in law enforcement has been widely supported in the United States, even though, there is no independent, comprehensive, scientific, peer-reviewed study of the overall effectiveness of DNA data banks in solving crimes.[3,15] Instead we have simple assertions, such as that of Senator Jon Kyl (R-AZ), one of the authors of a 2005 federal DNA act, that "We know from past experience that collecting DNA at arrest or deportation will prevent rapes and murders that would otherwise be committed."[12]

Only the 47 member states of the Council of Europe are bound by the ruling, but the ruling could nonetheless cause other countries and individual states to reexamine their policies. Most relevant in this regard are the conclusions of the Human Rights Court that simple assertions of the effectiveness of a DNA profile or sample in solving or preventing crime, or even terrorism, are not sufficient justification for the privacy invasion inherent in the bioidentifier data bank. Second, the collection and indefinite retention of fingerprints requires justification itself — and thus it should no longer be sufficient (if it ever was) to justify retention of DNA profiles because they are the same or substantially similar to fingerprints, as I have been guilty of doing myself.[16] Third, juveniles are a special case, and it will be extremely difficult to justify retention of any of their biomarkers, although there may be convictions of specific violent crimes that can provide that justification. Fourth, no matter how one comes out on the collection, storage, and use of fingerprints, photographs, and DNA profiles, there seems to be insufficient justification to ever retain DNA samples. Requiring their routine destruction after a DNA profile is created seems to be a case of "genetic exceptionalism," but it really is not. It is simply the recognition that the DNA molecule itself can be considered a medical record, and like an electronic medical record, can be read by a machine to disclose sensitive private information about people and their family members, unrelated to anything relevant to the criminal justice system.[16]

Biometric identifiers have complex privacy implications that demand much more rigorous analysis than they have received. Former Homeland Security Secretary Michael Chertoff, for example, may have been trying to deflect close analysis of the privacy aspects of fingerprints when he said during a Canadian press conference, "a fingerprint is hardly personal data because you leave it on glasses and silverware and articles all over the world, they're like footprints. They're not particularly private."[17] Of course, the same could be said about DNA samples: you shed them inadvertently, including leaving them on "glasses and silverware." In this respect, fingerprints should be treated, as the European court did, more like DNA samples than footprints. Jennifer Stoddart, the Privacy Commissioner of Canada, responded to Chertoff that, under Canadian law (as well as under the privacy policy of the U.S. Department of Homeland Security),[18] fingerprints are personal information, and she worried that the increasing reliance by the United States on the collection of biometric data in the name of national security and identifying suspected terrorists might lead Canada to lessen its standards of safeguarding personal information.[19]

All these issues should be subject to wide-ranging debate in the United States. It has, for

example, been suggested that one means of doing away with the racial and ethnic inequalities inherent in the current method of obtaining biometric information from arrestees is to have a universal criminal database that collects biometric information from everyone.[20] This suggestion, if implemented, could be viewed as converting a free country into a "nation of suspects."[16,21] It would not automatically make us a *1984* society in which all our conversations would be monitored and deviation from the government's line would be grounds for punishment, but it could radically alter the way we view ourselves and our relationship to our government. Nonetheless, whether such a universal system of DNA profiling would be acceptable to the Human Rights Court was not specifically decided.

The European Court of Human Rights is, I think, correct to emphasize the differences between democracies and police states as reflected in the types of personal information police are permitted to collect and retain about citizens. Each individual point of data may seem insignificant, but when data sets are merged, privacy is effectively destroyed. No one has made the privacy point better than Aleksandr Solzhenitsyn in his novel *Cancer Ward*, in which he writes that, in a totalitarian state, people are obliged to answer questions on a variety of forms, and each answer "becomes a little thread" permanently connecting him to the government:

> There are thus hundreds of little threads radiating from every man. . . . They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads . . . and for these people's authority.[22]

Bioidentifiers implicate privacy even more than answers on forms such as tax returns, because they identify us directly and can be seen as an integral part of us. When the police have and use DNA in investigations of criminal activity, the European Court of Human Rights seems correct to conclude that privacy is being invaded, and if the sources of that DNA are innocent of any crime, this use cannot be easily justified in a democratic society.

Mr. Annas reports being a board member on the Council for Responsible Genetics. No other potential conflict of interest relevant to this article was reported.

From the Department of Health Law, Bioethics, and Human Rights, Boston University School of Public Health, Boston.

1. S. and Marper v. The United Kingdom, [2008] ECHR 30562/04.
2. Wambaugh J. The blooding. New York: William Morrow, 1989.
3. McCartney C. The DNA Expansion Programme and criminal investigation. Br J Criminol 2006;46:175-92.
4. Williams R, Johnson P. Circuits of surveillance. Surveill Soc 2004;2:1-14.
5. Simoncelli T, Steinhardt B. California's Proposition 69: a dangerous precedent for criminal DNA databases. J Law Med Ethics 2006;34:199-213.
6. National Research Council. Bits of power: issues in global access to scientific data. Washington, DC: National Academy Press, 1997.
7. R (on the application of S) v. Chief Constable of South Yorkshire; R (on the application of Marper) v. Chief Constable of South Yorkshire, [2002] EWCA Civ 1275.
8. DNA and human rights: throw it out. Economist 2008;12:73-4.
9. Watching Big Brother. Nature 2008;456:675-6.
10. Sturcke J. DNA pioneer Alec Jeffreys: drop innocent from database. Guardian. April 15, 2009:1.
11. Keeping the right people on the DNA database: science and public protection. London: Home Office, May 2009. (Accessed June 18, 2009, at http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/dna-consultation?view=Binary.)
12. Hsu SS. New rule expands DNA collection to all people arrested. Washington Post. December 12, 2008:A2.
13. Cole SA. Fingerprint identification and the criminal justice system: historical lessons for the DNA debate. In: Lazer D, ed. DNA and the criminal justice system: the technology of justice. Cambridge, MA: MIT Press, 2004:63-89.
14. Duster T. Selective arrests, an ever-expanding DNA forensic database, and the specter of an early-twenty first-century equivalent of phrenology. In: Lazer D, ed. DNA and the criminal justice system: the technology of justice. Cambridge, MA: MIT Press, 2004:315-34.
15. Rothstein MA, Talbott MK. The expanding use of DNA in law enforcement: what role for privacy? J Law Med Ethics 2006; 34:153-64.
16. Annas GJ. Privacy rules for DNA databanks: protecting coded 'future diaries.' JAMA 1993;270:2346-50.
17. Swire P. Chertoff says fingerprints aren't 'personal data.' Washington, DC: Think Progress, April 16, 2008. (Accessed April 18, 2009, at http://thinkprogress.org/2008/04/16/chertoff-fingerprints/.)
18. The Privacy Office. Privacy impact assessment: official guidance. Washington, DC: Department of Homeland Security, 2007.
19. Letter to the Minister of Public Safety and Emergency Preparedness Canada. Ottawa: Office of the Privacy Commissioner of Canada, April 11, 2008. (Accessed April 18, 2009, at http://www.privcom.gc.ca/media/nr-c/2008/let_080411_e.asp.)
20. Kaye DH, Smith ME. DNA databases for law enforcement: the coverage question and the case for a population-wide database. In: Lazer D, ed. DNA and the criminal justice system: the technology of justice. Cambridge, MA: MIT Press, 2004:247-83.
21. Glantz LH. A nation of suspects: drug testing and the Fourth Amendment. Am J Public Health 1989;79:1427-31.
22. Solzhenitsyn A. Cancer ward. New York: Farrar, Strauss & Giroux, 1969.

Copyright © 2009 Massachusetts Medical Society.