

## **B455. "Why DNA Testing is Worth the Risk" Financial Times (May 10, 2004), p. 13.**

---

In the growing debate over the encroachment of science on privacy, the use of DNA testing presents both high risks to privacy and great potential for the public good. How widely should it be employed and how does one determine its limits? This depends largely on the extent to which a society can ensure proper accountability to minimize abuses of such vital information. This entails using both privacy-enhancing technologies (for example, audit trails and encryption) and several layers of accountability (not just by various ministries but also by parliament and the media).

Most conflicts between the protection of privacy and services for the common good, such as national security and public health, have a tilted profile that makes it relatively easy to form the proper public policy - but not always to sell it to the public. Trading medical records, for example, which banks could use to call in the loans of sick people and employers could use to avoid hiring people who had had a heart attack - a practice that was once common and is now banned in the US - is grossly invasive and does little public good. Banning such practices is readily justifiable.

In contrast, using cameras to record license plates (but not the drivers) for traffic violations can save lives and entails a minimal invasion of privacy. It should be an easy public policy to embrace.

The public policy profile of DNA testing and data banks is very different. The level of privacy invasion involved is high. Testing someone's DNA can reveal much about their ancestral history - say, family diseases and, arguably, their racial origins. It can determine whether one - or even one's siblings and children - is predisposed to still other debilitating illnesses. As reflected in the increasingly bitter nature of paternity suits, it is also used to determine who is and who is not the biological parent of a child.

From many aspects, however, the public benefits are tremendous. In its most commonly recognized role, DNA testing helps solve individual crimes when the criminal leaves, say, some hair or blood behind, which enables DNA comparisons with someone who can be reasonably suspected of having committed that crime. How widely the authorities should cast such a net is a matter of much controversy. Some would limit the suspects to only those the police can demonstrate would have reasonable cause to have committed the crime. Others would include a much larger range of suspects - for example, the residents of a whole village in which it occurred.

Accountability is the key. The stronger the legal assurances that DNA data collected by police will be used only for solving crimes - and remain inaccessible to unauthorized individuals including the media - the more widely authorities may cast the net.

DNA testing provides better opportunities than any other available tool to prove wrongly accused people innocent. Democratic societies like to believe they are committed to going to the limit to ensure innocent people will not be incarcerated, as reflected in the commonly held notion that it is preferable to let 100 criminals walk free than to jail one innocent person. DNA can serve justice very well indeed. Surely this alone would justify the development of extensive DNA data banks - including of those arrested and not just convicted - as long as the data banks are properly supervised?

In another increasingly important use of DNA technology, it can assist national security efforts by enabling identification of the bodies of terrorists. DNA testing could, in fact, be the

ultimate "identification card", if such a card is truly in the national interest. The data can also greatly help medical research, although in this case, it should be "de-personalized" - released to researchers without the names, addresses or other such attributes that enable personal identification. Researchers should commit themselves, subject to oversight, not to sidestep the ban against tracing people, even if it encumbers their work.

When it comes to weighing the considerable benefits of DNA testing against the growing demand for privacy protection, among the best technological safeguards is high-powered encryption of the data banks. Encryption could largely eliminate the possibility that unauthorized individuals will access information locked in these databases. Another safeguard can be provided by audit trails, in which anyone who accesses a file must leave their identification details. Audit committees should be established to review these trails. Separating DNA information from personal identifiers and requiring a court order for disclosure of names and addresses of those identified as criminals is crucial. Basic laws should determine the purposes for which these data banks may be used and should clearly ban other uses. For instance, parliaments should determine whether they may be used in paternity suits. A privacy advocate should be appointed whose duty would be to ensure the data are not abused. Regular oversight by non-partisan groups of lawmakers is part of good accountability. Annual reports about abuses that occur and corrective measures taken could help focus the public's attention. In the end, however, in a non-perfect world, it comes down to one question: Does one trust the various layers of accountability, or fear abuses to such an extent that one is willing to sacrifice the many advantages that DNA testing can bestow on society? I vote with those who hold that we can provide adequate accountability.

The writer is author of *The Limits of Privacy* and, most recently, *From Empire to Community: A New Approach to International Relations*; he is speaking on science and privacy tonight at the ICA, The Mall, London