A Communitarian Approach: A Viewpoint on the Study of the Legal, Ethical and Policy Considerations Raised by DNA Tests and Databases

Amitai Etzioni

A Communitarian Approach

This article seeks to outline a viewpoint on the study of the legal, ethical and policy considerations raised by DNA tests and databases (from here on, DNA usages). It does not delve into the specifics involved. It outlines a way of thinking that has proven productive elsewhere[1] and seems promising in dealing with DNA usages in the United States, but little more. Given that this essay is about a communitarian approach that draws on specific communitarian values, I turn next to briefly present the approach here followed.[2]

Communitarianism Defined and Disaggregated

Communitarianism is a social philosophy that maintains that society should articulate what is good, and asserts that such articulations are both necessary and legitimate. Communitarianism is often contrasted with classical liberalism, a philosophical position that holds that individuals should formulate their idea of good on their own. Communitarians examine the ways shared conceptions of the good (values) are formed, transmitted, justified, and enforced. Hence communitarians are interested in communities (and moral dialogues within them), historically transmitted values and mores, and the societal units that transmit and enforce group values such as families, schools, and voluntary associations (social clubs, churches, and so forth), which are all parts of communities.

Although all communitarians uphold the importance of the social realm, and of community in particular, they differ in the extent to which their conceptions are attentive to liberty and individual rights. Early communitarians, such as Ferdinand Tönnies and Robert Nisbet, stressed the importance of closely knit social fabric and authority. Asian communitarians are especially concerned about the values of social order. They argue that to maintain social harmony, individual rights and political liberties must be curtailed. Some seek to rely heavily on the state to maintain social order (for instance, leaders and champions of the regime in Singapore and Malaysia), and some on strong social bonds and moral culture (as Japan does). Asian com-

Amitai Etzioni, Ph.D., *served as a Senior Advisor to the Carter White House; taught at Columbia University, Harvard Business School, Berkeley, and serves as University Professor at George Washington University. He served as the President of the American Sociological Association, and he founded the Communitarian Network. A study by Richard Posner ranked him among the top 100 American intellectuals. He is the author of* The Active Society, Genetic Fix, The Moral Dimension, The New Golden Rule, *and* My Brother's Keeper. *His latest books are* The Common Good, From Empire to Community, *and* How Patriotic is the Patriot Act: Freedom.

munitarians also hold that the West's notion of liberty actually amounts to anarchy, that strong economic growth requires limiting freedoms, and that the West uses its idea of legal and political rights to chastise other cultures that have inherent values of their own. In 1995, Alan Ehrenhalt's book, *The Lost City: The Forgotten Virtues of Community in America,* questioned the value of enhancing choice achieved at the cost of maintaining community and authority. In the 1980s, Charles Taylor, Michael Sandel, Michael Walzer, and Robert Bellah and associates criticized the excessive individualism of classical liberalism exemplified by the United States under President Reagan, and in Britain under Prime Minister Margaret Thatcher.

My version of communitarianism, laid out in my book *The New Golden Rule,*[3] holds that the good communitarian society has two key elements: a carefully crafted balance between liberty and the common good as well as between individual rights and social responsibilities, and a social order based as much as possible on moral persuasion as opposed to coercion. Both point to the quest for common ground. The second element is of special import for the issues at hand. It suggests an approach to policymaking and ethical deliberation that differs sharply from a notion that governs our legal system and often spills into our policy and ethical arenas – the notion that the best way to proceed is for two extreme advocates to present a case, one from each side. (The ultimate example of this approach was the CNN show, *Cross Fire*). Each side makes its case in the most extreme possible way, and from the clash of these polarized positions somehow justice, fairness, and an acceptable policy is to arise. This tendency has been evident in the debate about rights and national security in the age of terrorism: one side argues that our constitution is being shredded, and the other argues that questioning new security measures aids and abets the enemy.[4] Some signs of such polarization are found between those who view practically all new uses of DNA tests – especially DNA databases – as endangering individual rights, and those who view them as greatly advancing the common good. From my neocommunitarian viewpoint, the basis of all such legal, policy and ethical deliberations should be that there is no one value that *a priori* trumps all others; that typically, a common ground needs to be and can be found most effectively through dialogue, not through confrontation.

The Fourth Amendment as a Communitarian Concept

The communitarian concept I just outlined is reflected in the legal concept outlined in the Fourth Amendment. The law distinguishes between reasonable searches, those in which there is a compelling public interest – and unreasonable ones, those in which the right to privacy prevails. To stress this point, one should contrast the texts of the First and Fourth Amendments. If the Fourth were to be written in the same strongly right-privileging language as the First, it might read, "Congress shall make no law..." allowing searches and seizures. (Note that I am referring to the idea contained in the original text, and not to the numerous court cases that have taken place over the centuries and their accumulative – and modifying – effects on the way the Fourth Amendment has been viewed over the years.) The Fourth Amendment's further requirement that "no Warrants shall issue, but upon probable cause, supported by Oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized" provides a mechanism for sorting out when searches are unreasonable or reasonable. Most importantly, that which is considered reasonable changes as the social climate changes. Thus, in response to the rise of radical individualism, the erosion of authority, and above all, new threats to the common good (especially to homeland protection) the courts have expanded the realm of reasonable search and seizure, specifically in the Patriot Act. For instance, more legal searches have occurred for which neither warrants nor even specific suspicion is required. Examples include screening gates in airports (introduced in 1973), searches of backpacks in New York City subways (in 2005), and gradually over the decades by one state at a time drug testing for specific professions such as train engineers, road-side sobriety checkpoints,[5] and the kind of DNA testing that involves a sweep of innocent people (a whole village, for example) in order to try to locate a criminal, the process of which has

Indeed, much of what was considered unreasonable before the September 11, 2001 attacks has become reasonable in the past couple of years. But, as no attacks have since occurred, some of what had become reasonable was again considered unreasonable when the Patriot Act came up for renewal at the end of 2005.

already taken place in the United Kingdom but as far as I can establish not yet in the United States.

Indeed, much of what was considered unreasonable before the September 11, 2001 attacks has become reasonable in the past couple of years. But, as no attacks have since occurred, some of what had become reasonable was again considered unreasonable when the Patriot Act came up for renewal at the end of 2005. DNA searches once considered matters of science fiction and entirely unreasonable are now becoming reasonable. As their service to the common good becomes better known, their intrusiveness declines (for example, the shift from blood tests to swabs to collect samples), and their usage becomes more widespread.

Preventive Collections?

Even for those who view the recent trend in democratic societies to treat new security measures as reasonable, one measure is particularly difficult to consider as legitimate and particularly relevant to the application of DNA usages. Since September 11, 2001, the FBI has been explicitly instructed to shift its focus, when dealing with terrorism, from prosecution to prevention.[6] It is widely recognized that it makes little sense to try to prosecute suicide bombers after attacks such as those on the World Trade Center and that the threat of such prosecution is unlikely to deter them. In either case, an unacceptable level of damage will be done if one waits until a terrorist attack occurs before one acts.

At the same time, one must recognize that a shift from prosecution to prevention often entails harassing a large number of innocent people. To prevent attacks, one must question and search the property and communication of a large number of people (selected for example on the basis of their country of origin), most of whom have not committed any crimes, and show no sign of planning to do so. A typical example is the invitation issued to 5,000 Iraqi Americans in the Detroit area at the eve of the 2003 invasion of Iraq to come for an interview at FBI offices. They were "invited" merely because of their country of origin and because they were males of a certain age, but not because of any specific suspicion. Such an invitation is a chilling experience for most people, especially as they realize that declining to interview will turn them into suspects.

Collecting DNA from people who have not committed a crime in order to have it on file for the future identification of a criminal is similarly preventive. Requiring innocent people to provide DNA samples – for example when applying for a passport or driver's license – when not provoked by a criminal search is an even more invasive situation than testing an entire community in search of a specific criminal. In the latter case, testing may be justified as a crime has been committed by someone in the vicinity. In preventive collection, one assembles the DNA of a large number of people without the claim that any of them did anything illegal. In the case of a post-crime DNA sweep, DNA of all who are cleared can be destroyed; in preventive collections, DNA is stored for the foreseeable future.

An important lesson can be gleaned from the internment of Japanese people in America during World War II. One of the strongest legal criticisms of interning *all* Japanese-Americans was that the approach was both over-inclusive and under-inclusive. It was over-inclusive because it undoubtedly included Japanese-Americans who posed no threat to this country. It was under-inclusive because it did not include other possibly disloyal citizens of other ethnicities and national origins (for example, German-Americans). Obtaining DNA from those visiting the US (some 300 million a year, not a mean task), and maybe even from all US citizens, for storage in a databank bears the same problems. It will be over-inclusive because it will store DNA data of many scores of millions of innocent people. At the same time, the databank will be under-inclusive, because it will leave out many millions of illegal immigrants.

As of yet, the US has no universal DNA database. Inclusion is mostly limited to convicted individuals, although some states (and possibly the Federal Government) are moving to take DNA samples from arrestees. The military also uses DNA samples to identify soldiers killed in action. Britain, however, *is* moving toward a universal bank. To the extent that the law and order system in America is shifting its focus from prosecution to prevention, we should expect to see America move closer toward the British approach. At the very least, we should expect to see databanks that include millions of innocent people, even if those databanks are not fully inclusive.

To conclude whether or not population-wide DNA databases are justified, we need to learn much more about the extent to which such databanks are truly useful in preventing terrorist attacks, and the extent to which their threat to privacy can be minimized. These questions largely remain to be explored and prevent a summary judgment here. Also important to keep in mind is that these banks may well cost so much that the same resources could be much more effectively employed elsewhere.

Balancing Intrusion and Service to the Common Good

In previous publications, I have tried to take the quest for the criteria of establishing the proper balance between individual rights and the common good in a different direction. In a study of privacy,[7] I suggest that

there is no need to consider limiting privacy unless *not* doing so poses a serious threat to the common good. Other means of coping with a threat to the common good ought to be tried first, and – if some limits on privacy are nevertheless needed, they should be as minimally intrusive as possible. Following this scheme, I found that judgments have come relatively readily. In some cases, a proposed course of action that requires little intrusion was highly necessary to safeguard the common good. Other situations had clearly the opposite profile: the intrusion they called for was immense while the contribution of the intervention to the common good was minimal.

For example, in the realm of medical privacy, if a person has a stroke, some banks that find out will call in their loans. There is little or no contribution to the common good in such interventions, but the intrusion is very high, indeed one of the highest intrusions one can imagine. An opposite example concerns surveillance cameras in public spaces on campuses where there have been several rapes. Assuming that notices are posted about the installation of the cameras and the use of the cameras is properly supervised, the cameras are minimally intrusive. To the extent that these cameras reduce rapes, and that no other even less intrusive but effective solutions are available, these cameras seem reasonable. (Note that closed-circuit television [CCTV] security cameras in the UK have been criticized as useless and intrusive,[8] but turned out to play a key role in identifying the 2005 subway bombers.) Whether or not one agrees with these assessments, they illustrate my suggestion that balancing the scope of an intrusion with its corresponding impact on the common good is *one* consideration that should be employed in determining reasonable limits on privacy.

DNA usages are more difficult to assess from the viewpoint of the criteria just outlined because they are often both highly intrusive, and can contribute much to the common good. Whereas one of the examples cited above was highly intrusive and contributed little if anything to the common good (high/low), and the other example just the opposite (low/high), many DNA usages are often highly intrusive and highly desirable (high/high). As such, it is more difficult to read the scale and determine where a proper balance lies. We must take a closer look. Accordingly, I next examine the level of intrusion as well as the contribution to the common good of select DNA usages.

Intrusion

The use of DNA is highly intrusive because DNA can reveal much more about a person than a picture of a face (as captured on surveillance camera), a license plate (as seen on a traffic camera), an identification card (as registered on traditional passports, distinct from those that use biometrics), and even a set of fingerprints. Moreover, DNA discloses information about our family members and ancestors. DNA is also highly accessible. We leave traces of our DNA in public all the time, whether it be in shed hair, skin, or saliva left on coffee cups or cigarettes, etc. DNA can be extracted and tested entirely unbeknownst to us. Authorities are also quite able to conceal that these tests have taken place. Not many intrusions are as invasive, and at the same time as easy to accomplish and conceal

There are a number of factors that will work to mitigate the intrusiveness of DNA usages, at least in the near future. It is true that we can divine very specific information from DNA – for example the color of one's hair, or whether one is susceptible to certain diseases – but it will take a considerable number of years before authorities will be able to look at the genetic code and piece together a composite picture of a human being. Thus, whereas one's DNA has the *potential* to reveal an enormous amount of information regarding a person, at this stage authorities are unable to identify enough genes, their functions, or their expression patterns to *actually* reveal the information.

Additionally, proponents of DNA databases argue that the DNA profiles kept and stored by law enforcement – the thirteen STR loci – do not provide any meaningful information about individuals, aside from allowing us to determine whether two samples have come from the same person. STR is an abbreviation for short tandem repeat polymorphisms, which are distinctive parts or samples of a person's DNA. The FBI has chosen a set of thirteen such samples (the thirteen STR loci) as a recording standard for its database. When a piece of DNA is found at a crime scene, it can be matched to a particular person's thirteen STR loci (if that person is in the database). Thirteen STR loci thus act a bit like fingerprints for identifying DNA. Indeed they are said to be no more intrusive than fingerprints. For by themselves, the thirteen STR loci cannot tell us what the person looks like or anything about their ancestry or susceptibility to disease. This point, however, should not be overestimated.

One may argue that once the DNA has been "fingerprinted" and the thirteen STR loci have been typed and entered into a database, presumably the DNA samples are no longer needed. The thirteen STR loci allow the police to match a sample, but they do not disclose much meaningful information about the individual. However, the DNA *samples* do contain *much* information about the individual – his family, history, predispositions etc. Hence privacy advocates argue that even if there are safeguards regarding access to the DNA samples, keeping this potent information around is a

risk that should not be taken. Temptation of authorities to misuse or abuse the information is too great. Hence the samples should be destroyed once the STR loci have been extracted.

The problem with this argument is that there *are* instances in which the entire DNA sample is needed, such as when settling claims that testing was inappropriately conducted. Also, DNA tests have become more discerning over the years, and are likely to become so in the future. That is, the authorities will be able to derive more information about the person whose DNA sample they found at the crime scene or elsewhere. Hence, being able to return to the samples for further testing is of clear value to the common good and to individual rights. At the same time, there is no denying that databases containing the original samples are potentially much more intrusive than limited DNA profiles.

The claim, however, that extremely unreliable eyewitness testimony and extremely reliable DNA evidence *are* the same because they both can be misinterpreted is spurious.

In short, although the intrusiveness of DNA usages *can* be reduced, it is currently nevertheless substantial, and much of its intrusiveness is dependent on future developments in science and technology.

Contributions to the Common Good

While banking DNA information entails a high level of intrusion, it also provides large contributions to the common good. For the last two decades, DNA tests and databanks have been the most powerful tool available to police and prosecutors investigating new crimes, solving old crimes, locating suspects, and indicating when authorities are on the wrong track. DNA tests are many thousand times more accurate than eyewitness testimony often relied upon to identify suspects and convict people. Walter Rowe, a leading academic forensic scientist, has gone even further, saying that DNA testing "may be the greatest advance in forensic science in history."[9] As tests and databanks are expanded, the benefits of DNA usages will be still greater.

There seems to be no data on the deterrence effect of DNA usages. However, as it becomes increasingly known to the public that a criminal can be identified if he or she leaves behind even one hair or drop of sweat, it would be surprising if this has no impact on deterrence. Indeed an early commentator on criminal punishment, César Becaria, argues that deterrence varies more across the likelihood of detection and punishment than it does across the amount of punishment. In plain English, it matters more how likely one is to be caught than how big the penalty is going to be. Following his argument, increased use of DNA in criminal justice would increase deterrence more than harsher sentencing would. It is hence likely that DNA usages will lead not only to more accurate convictions, but also to lower overall crime rates, which is of course a very desirable outcome. In short, benefits of DNA banking to public safety are substantial.

Further, DNA tests and databases help *protect* individual rights. One of the strongest, and indeed noblest, claims of free societies is that it is better to let a thousand guilty people go free rather than imprison just one innocent person. This is a very powerful conviction attesting to how abhorrent free societies hold the incarceration of the innocent. Extensive and accessible DNA testing and databases can be strongly justified on this ground alone: as of 2003, DNA tests have exonerated 130 people falsely convicted and incarcerated. Twelve of these people walked off of death row. Unfortunately for some, the tests come too late. Frank Lee Smith, convicted in 1985, died of cancer on death row in 2000, waiting for DNA testing that would exonerate him but was completed only eleven months later.[10]

Moreover, by making it possible to quickly identify the guilty person from among a group of suspects (a process to be much further accelerated if handheld, quick response DNA tests become available[11]), DNA usages greatly reduce the humiliation and costs entailed in being a suspect in a police investigation. (In one case in which data on this point is available, namely in Virginia, we find that DNA analysis routinely eliminates twenty-five to thirty percent of suspects in police investigations).[12] Thus if one compares the use of DNA tests to identify a perpetrator relying on eyewitnesses and police line-ups, which are notoriously unreliable,[13] one sees the double virtue of DNA testing and databases: they vastly enhance the probability that those who are guilty will be convicted, and those who are innocent will be rapidly cleared.

Consider the following situation, based on an actual occurrence. A rape occurred in a hospital. Eleven people had ready access to the victim's room overnight. Before DNA tests were available, the police would have quite legitimately questioned all eleven people – asking them to provide alibis, checking their records for past offenses, and interviewing their supervisors, friends and family members. If the rapist was not identified, the case might go unsolved for years; none of the suspects would be cleared and a cloud would hang over

them at work and in their community despite the presumption of innocence guaranteed in trial court, but not in the court of public opinion. In the near future world of rapid DNA testing, the police could simply ask each of the eleven to provide a sample of saliva or a hair, and all but one suspect would be cleared in short order, without the undesirable effects of public speculation as to their guilt.

Some defense attorneys who recognize that DNA testing has the merit of quickly determining who is not a suspect nevertheless argue that this feature poses a problem. These attorneys agree that eyewitness identifications are notoriously unreliable, and point out that juries nonetheless give a disproportionate amount of weight to them, leading to numerous wrong convictions. They fear, however, that DNA evidence is becoming the new eyewitness evidence. If a biological sample has been found at the crime scene, and the DNA matches that of the defendant, juries may take that as a 100% reliable indicator of the defendant's guilt, even though the DNA evidence is only reliable in determining whether the defendant was present at the crime scene.

Take, for example, a rape prosecution. A semen sample was collected from the victim and the crime scene. The DNA matches that of the defendant. All that the DNA test proves is that the defendant and the victim engaged in sex.[14] The DNA test does not reveal guilt as to the rape charge, however, because the sex may have been consensual. Yet, defense attorneys worry that juries may take the DNA test results as conclusive proof that the defendant is guilty of rape.

As I see it, however, one confuses two issues here. DNA tests are many thousand times more reliable than eyewitness testimony. In *both* cases all that the evidence can claim to indicate is that the suspect was on location; the suspect is still subject to additional arguments and evidence. Like eyewitness testimony, DNA evidence can be misinterpreted. The claim, however, that extremely unreliable eyewitness testimony and extremely reliable DNA evidence *are* the same because they both can be misinterpreted is spurious.

More serious problems concern the possibility of carelessness or corruption of those who perform the tests. There have been a handful of cases in which mismatches occurred due to mishandling of the samples in labs, and other such errors. There have been a number of high profile cases in which crime labs have purposely falsified data in order to secure a conviction. Fred Zane, a serologist in a West Virginia crime lab, falsified DNA data over a number of years, throwing into question all the cases for which his data was used.[15] There were also serious problems in FBI crime labs.[16] It follows that we must stress that although there is a great potential that DNA evidence will be used for "good" – convicting the guilty and exonerating the innocent, there is also the potential that it can be used for "evil" – falsifying evidence to secure convictions or to frame innocent people. The threat of negligent or incompetent lab work also cannot be overlooked.

In summary, like most other technologies, whether DNA usages are "good" or "bad" (in terms of serving the common good) depends upon the motives and actions of those in control of the tools. In this case, when the chain of evidence is carefully vetted, one at least knows that the tool itself is reliable. In the case of eyewitness testimony, often even if all the police and attorneys have conducted themselves in an exemplary manner, we still have unreliable information.

In short, DNA usages do make major contributions to the common good by facilitating crime solving, likely increasing deterrence, reducing the burden on suspects, and proving the innocence of the wrongly convicted.

Hi/Hi Profile and Accountability

To recap the argument thus far: In assessing DNA usages or any other such new measures or technologies, the communitarian approach here followed does not grant, *a priori,* the right of way to either the common good or to individual rights. Hence when a measure is highly intrusive and makes little contribution to the common good, it ought to be barred. And if a measure has the opposite profile, it should be embraced. Both statements are subject to many other considerations not explored here – for instance, relative costs, the extent to which the same results can be achieved by voluntary means, and so on. But how should one deal with measures (henceforth referred to as hi/hi measures) that are highly intrusive as well as make major contributions to the common good, including individual rights? One may of course seek to reduce intrusiveness, but judgment must still be made at a point in time in which the level of intrusiveness is given and considerable.

To make my next point, I return to the use of security cameras [CCTV] in London subway stations that helped to identify the London subway bombers in 2005. CCTV footage, which could have illuminated more facts regarding the shooting death of Brazilian man Jean Charles de Menezes at the hands of UK police in the London subway, has gone "missing." London tube workers claim that the CCTV cameras were working when Menezes was shot by police, yet the police claim the opposite. Many suspect a police cover-up regarding the killing of a man who turned out to be innocent.[17] This questions our trust in those conduct-

ing surveillance, not the reliability or reasonability of CCTV.

Placing a tool as powerful as DNA databases and testing in the hands of the police is clearly an effective crime-fighting tool, but it requires the introduction of stronger monitoring of the police, including a national civilian review board. Before further explaining this review board, however, it is necessary to discuss in more general terms how supervision and accountability are best ensured.

The discussion thus far, as often is the case in other such deliberations, has focused on determining what is reasonable and where the proper balance lies between individual rights and contributions to the common good. To complete the judgment as to whether or not a given new measure that enhances the powers of public authorities is called for, I suggest that a second form of balancing needs to be considered which concerns not whether the government should be accorded new powers, but how closely it is held accountable regarding the ways it uses these powers. From this viewpoint, the key issue is not if certain powers – for example, keeping DNA samples – should or should not be available to public authorities, but whether or not these powers are used legitimately, and whether mechanisms are in place to ensure such usage. The balance sought here is not of public interest and rights, but is of the supervised and the supervisors, and their superiors. Deficient accountability opens the door to government abuses of power. Excessively tight controls, however, can also cause harm. Thus, a case can be made that in the decades preceding the Church Committee, under most of Hoover's reign, the FBI was insufficiently accountable, but that after the Committee's rules were institutionalized, until 9/11, the FBI had excessive limits on its power. It follows that a carefully calibrated and judicious accountability system makes the introduction of hi/hi measures tolerable.

Some accountability is built into any organizational set of rules, regulations, and supervisory layers, as it is in various police departments and national security agencies such as the NSA, FBI, and the new Department of Homeland Security. In addition, federal agencies have offices of Inspectors General which have in the past, in several cases, issued reports that were quite critical about the government's conduct and demanded corrections. The courts also provide a measure of accountability, with the Supreme Court acting as the ultimate arbitrator.

Under the American system of checks and balances, Congress is supposed to oversee the work of the executive branch, and has several instruments for doing so. These include requiring heads of agencies and other high ranking officials to respond to written questions, testify before congressional committees, and turn over documents; conducting hearings in which civil libertarians and others can make their case; ordering the General Accounting Office to conduct a study; and more. A survey of the extent to which Congress provides an effective layer of accountability regarding DNA usages is well beyond the scope of this article. However, given the fact that members of Congress are under constant pressure to raise funds, do the special bidding of their constituents, and vote on many hundreds of bills each year, and given the ease with which the executive branch in the past has often escaped proper scrutiny, I conclude that an additional source of accountability is needed for hi/hi measures like DNA testing.

The ultimate source of oversight is the citizenry, informed and alerted by a free press and civil liberties advocates, and briefed by public authorities about their needs. Both the press and various libertarian groups have been very active in alerting the public to the dangers of biological data banks and DNA testing and profiling, and arguing in favor of various limitations on DNA usages. To help focus and institutionalize public scrutiny, I favor an independent public accountability board, composed from public figures with known integrity and who command security clearance (Lee Hamilton and Tom Kean, vice-chair and chair of the 9/11 Commission, and Paul Volcker, the former chairman of the Federal Reserve could so serve). The board would act much like local civilian review boards that have formed in some sixty percent of our nation's largest cities where the public sought to keep an eye on the police after widespread corruption and abuse was revealed. The board would regularly visit different DNA testing facilities and issue an annual report stating the extent to which the board found that the various agencies complied with the various safeguards on the DNA usages passed by state and national legislature, and whether such safeguards sufficed. For instance, are audit trails (which determine who accesses the databases) in place? Are those trails routinely reviewed to determine if unauthorized people have queried the databases and used the information for illicit purposes? If such instances were found, were corrective measures taken?

Those who find such a board unlikely to be tolerated or able to do its job should look at the 9/11 Commission. Indeed if the 9/11 Commission could be re-implemented it could serve as such an accountability board not only for DNA usages. It would likely be much more effective than the Civil Rights and Privacy Board included in the Department of Homeland Security. As with civilian review boards of local police, opposition to the formation of a national civilian review board to monitor hi/hi measures, of which DNA usages are

only one example, may well be one indication that the system may be tilting too far toward concerns about the common good and may not be sufficiently concerned about individual rights.

Acknowledgements

I am indebted to Seth Axelrad for extensive research assistance and Kristen Bell for extensive editing assistance. This article was supported by a grant from NIH (R01-HG002836).

References

1. See A. Etzioni, *The Moral Dimension* (New York: The Free Press, 1988), and A. Etzioni, *How Patriotic is the Patriot Act?: Freedom versus Security in the Age of Terrorism* (New York: Routledge, 2004).
2. For a fuller description of this kind of communitarianism, see A. Etzioni, *The New Golden Rule* (New York: Basic Books, 1996).
3. *Id.*
4. For more on this point, see A. Etzioni, *How Patriotic is the Patriot Act? supra* note 1.
5. For further examples of such warrantless, suspicionless searches that have been ruled permissible under the Fourth Amendment, see M. Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution," *University of Pennsylvania Law Review* 143 (1995): 824-25.
6. For more on this point, see A. Etzioni, *How Patriotic is the Patriot Act? supra* note 1.
7. See A. Etzioni, *The Moral Dimension, supra* note 1.
8. See J. Rosen, "A Watchful State," *The New York Times Magazine,* October 7, 2001, at 38ff. Also, J. Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (New York: Random House, 2004).
9. K. Jost, "DNA Databases," *The CQ Researcher* 9, no. 20, May 28, 1999. *Available at* <http://library.cqpress.com/cqresearcher/cqresrre1999052800> (last visited February 16, 2006).
10. L. Romano, "When DNA Meets Death Row, It's the System That's Tested," *The Washington Post,* December 12, 2003, at A1.
11. K. Flynn, "Fighting Crime with Ingenuity, 007 Style: Gee-Whiz Police Gadgets get a Trial Run in New York," *New York Times,* March 7, 2000, at B1.
12. Interview: Dr. Paul Ferrara, Director of Virginia Division of Forensic Science, "Discusses Gathering of DNA Evidence," *All Things Considered,* National Public Radio, July 27, 2000.
13. It has been widely documented that eyewitness accounts are unreliable. As Justice Brennan wrote in his opinion in *United States v. Wade,* "The vagaries of eyewitness identification are well known; the annals of criminal law are rife with instances of mistaken identification." Gary L. Wells and Eric P. Seelau summarize findings regarding eyewitness identification: "Although there is no way to estimate the frequency of mistaken identification in actual cases, numerous analyses over several decades have consistently shown that mistaken eyewitness identification is the single largest source of wrongful convictions." G. L. Wells and E. P. Seelau, "Eyewitness Identification: Psychological Research and Legal Policy on Lineups," *Psychology, Public Policy and Law* 1, no. 4 (1995): 765-791.
14. Even this cannot be assumed with full confidence given that in a few instances rapists have intentionally left other people's semen behind.
15. National Public Radio, "Crime Labs under Scrutiny around the US for Producing Evidence that Wrongly Convicts People for Felonies," *Weekend Edition,* May 12, 2001.
16. The Office of the Inspector General reported that FBI employee Jacqueline Blake falsified lab documents. The report also lists and explains several vulnerabilities in the FBI lab's protocol and practice. Office of the Inspector General, The FBI DNA Laboratory, *A Review of Protocol and Practice Vulnerabilities,* May 2004. *Available at* <http://www.usdoj.gov/oig/special/0405/index.htm> (last visited February 10, 2006).
17. R. Cowan and D. Hencke, "Row over 'blank' CCTV tapes at station," *The Guardian,* August 23, 2005, at 8.