THE CASE FOR NATIONAL DNA IDENTIFICATION CARDS

Foes of the United States have demonstrated their ability to strike at the heart of this country. Fear of renewed attacks and a desire for greater national security have now prompted many to call for improvements in the national personal identification system. In particular, the possibility of a national identification card containing the carrier's DNA information is being seriously considered. However, this raises difficult questions. Would such a card system, and the extraction of individuals' DNA it entails, violate the 4th Amendment of the Constitution? This article will show that such a card system could in fact be found to be constitutional under the law of privacy as it stands today.

Introduction

National Identification Cards

Ever since September 11, 2001, the U.S. has remained on alert. More attacks are likely, according to the White House. Vigilance is required. The apparent ease with which the hijackers entered the country and integrated into American society prior to their strike has forced the national security authorities to reevaluate their methods. How can terrorists in our midst be identified, and further attacks prevented?

The current identification system, based on the social security number, driver's license and signature, is no longer adequate.[1] The U.S. now needs a foolproof identification system to avert the threat within its borders. One step towards this goal is illustrated by the Driver's License Modernization Act of 2002,[2] which would allow for cards with computer chips to carry "not only fingerprint information but other data, ranging from medical data to credit-card numbers - security and e-commerce on one piece of plastic."[3] Similar ID cards, carrying biometric[4] information and targeted exclusively at improving the effectiveness and efficiency of the national identification process, are being considered for the near future.[5]

---

[1]Solveig Singleton, *Biological ID Technology Can Aid Privacy*, 85 CONSUMERS' RESEARCH MAG., Issue 3 (2002), *available at* 2002 WL 14817440.
[2]Issuance of Drivers' Licenses Act, H.R. 4633, 107th Cong. (2001).
[3]Steven Levy, Adam Rogers & Mark Hosenball, *Playing the ID Card; Americans Have Never Had to 'Show Papers' to Move Around. Now They Must Choose Between Privacy and Security,* NEWSWEEK, May 13, 2002, *available at* 2002 WL 7294218.
[4]Biometric information is defined as information relating to the statistical analysis of biological observations and phenomena.
[5]*Arkansas Company's DNA Card Gaining Attention*, AP NEWSWIRES, Nov. 11, 2001.

DNA data

A card containing biometric information relating to fingerprints, while certain to be somewhat controversial, could in all likelihood be introduced without too much public opposition. Relinquishing your personal fingerprint information seems a small price to pay in the fight against terrorism.

But fingerprints are only the first step. Indeed, even Alan Dershowitz, a Harvard law professor known for his liberal opinions on a variety of issues, has recently argued that the state should create a "near foolproof system of identification using fingerprints, or for even greater accuracy*, DNA information*."[6] Most Americans would not, in his opinion, be averse to disclosing the information required by such a scheme and seeing that information accumulated in vast databanks, despite the loss of privacy this entails.

Scope of the scheme

DNA databanks of the sort at issue here have been around for a while. U.S. law enforcement authorities began building DNA databases in the early 1990s.[7] At first, only individuals convicted of serious criminal sexual crimes were listed. Nowadays, however, the scope of the databases has been broadened in many states to include data on individuals convicted of murder, violent felonies, and in some states, misdemeanors. The trend is for a relentless expansion of the scope of such information banks: bills have now been introduced in several states to broaden the scope of the databases to include arrestees.[8]

Opponents of the card scheme proposed by Mr. Dershowitz insist that the scope of the suggested DNA identification system should be limited.[9] Some argue, for example, that the scheme should only include individuals entering the country, or people with a criminal record. However, an identification system applying only to a small cross-section of the population would be of little use for national security purposes, and would inevitably lead to racial profiling and unfair singling out of specific minorities.[10] A nationwide card system therefore seems most appropriate under the present circumstances.

---

[6]Alan Dershowitz*, Identification Please*, BOSTON GLOBE, Aug. 11, 2002 at 14, *available at* 2002 WL 4142755 (emphasis added).
[7]David H. Kaye, Michael Smith & Edward J. Imwinkelried*, Is a DNA Identification Database In Your Future?,* 16 CRIMINAL JUSTICE 4, 4 (2001).
[8]*Id.*
[9] *See* Mark Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks,* 67 BROOK. L. REV. 127, 158-9, 165 (2001).
[10]Kaye, Smith and Imwinkelried, *supra* note 7, at 8.

Unpredictable public perception of the scheme

Whereas the institution of a national identification scheme based on fingerprint information seems relatively non-controversial, a DNA card system might prove a little more problematic. First of all, the reaction of the American public to such a scheme is as yet fairly unpredictable. Members of Congress themselves, when questioned on the issue, have remained decidedly non-committal, perhaps choosing to sit on the fence until the public reaction to the plan becomes clearer.[11] In addition, a host of thorny legal issues are sure to arise in connection with this identification scheme.

This iBrief will address the relevant privacy issues raised by the card system and the DNA extraction and isolation processes it entails. The author will attempt to show that, despite his personal misgivings with regards to such a system, the scheme championed by Mr. Dershowitz may be found to comply with the 4th Amendment of the U.S. Constitution.

Discussion

Fourth Amendment

The constitutional privacy standard is set by the 4th Amendment of the U.S. Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[12]

Would the DNA sampling required for the scheme constitute a search under the 4th amendment ?

"The Fourth Amendment requires that searches and seizures be reasonable."[13] Obtaining and examining evidence may constitute a search "if doing so infringes an expectation of privacy that society is prepared to recognize as reasonable."[14]

Here, the DNA extraction and isolation process necessary for the card system would undoubtedly constitute "obtaining and examining evidence." As will be shown below, however, this obtention of evidence might be found not to infringe upon any expectation of privacy that society regards as reasonable.[15]

---

[11] *See* AP NEWSWIRES, *supra* note 5.
[12] U.S. CONST. amend. IV.
[13] City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000).
[14] Skinner v. Railroad Labor Executives' Ass'n, 489 U.S. 602, 616 (1989).
[15] *See id*.

If that is indeed the case, the procurement of DNA evidence needed for the card system would not call into play the protections of the 4th Amendment. That is, even though the DNA extraction procedure might constitute a search under the common meaning of the term, it would not qualify as a "search" under the Constitution.

Here, neither the nature of the information gleaned (DNA code) nor the method of extracting the DNA would lead to the conclusion that the public's reasonable expectation of privacy would be violated.

1. Nature of the information

The Supreme Court, in *Katz v. U.S.*, held that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[16] This has been used, for example, to prove the constitutionality of face-recognition security systems comprising databases of individual faces. The argument runs as follows: you show your face in public, therefore a profile of it may be stored in a database for future recognition, because an individual has no reasonable expectation of privacy with regards to his facial features.[17]

DNA information is in some ways analogous. Our body constantly sheds cells, and in particular, skin cells. The DNA carried by these cells can be collected and isolated without difficulty, and the information it carries decoded.[18] Police forces, for example, have long been able to extract cells from a crime scene, by collecting hair follicles or bodily fluid deposits for example. These can then be made to relinquish their DNA, which, after being amplified, can be used to detect similarities with known DNA sequences, thus allowing for personal identification.[19]

Our DNA information is thus to a certain extent readily available to extraction and isolation. It is therefore arguable that the public has no reasonable expectation of privacy with respect to DNA information.

---

[16] Katz v. U.S., 389 U.S. 347, 351 (1967); *see* Mark Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks,* 67 BROOK. L. REV. 127, 134-35 (2001).

[17] *See* U.S. v. Dionisio, 410 U.S. 1, 14 (1973)

[18] *DNA Fingerprinting; Can Blood Found at a Crime Scene Really Identify a Criminal?, available at* http://www.darylscience.com/DNAFingerprinting.html (explaining the methods of DNA isolation from small cell samples).

[19] *See* Baechtel et al., *Panel Two: Criminal Law and DNA Science: Balancing Societal Interests and Civil Liberties,* AM. U. L. REV. 400, 421 (2002) ("It's almost impossible to not leave some genetic legacy of yourself behind everyday.")

If there is no reasonable expectation of privacy with regards to one's DNA information, the obtention of that information will not constitute a search. The DNA card scheme at issue here would not therefore come under 4th Amendment scrutiny.

2. Method of information extraction

Even if the mere collection of DNA information is not found to violate the public's reasonable expectation of privacy, opponents of the card scheme might argue that the extraction procedure itself would violate the reasonable privacy expectation, thus invoking the protections of the 4th Amendment.

This argument would not be valid today. Modern DNA sampling methods no longer violate reasonable societal expectations of privacy. Traditionally, DNA samples were obtained using buccal swabs: the inside of the individual's mouth was rubbed with a cotton wad, from which the cells necessary for the DNA extraction process were isolated.[20] Most courts found such a method to constitute a search, bringing the entire procedure under 4th Amendment scrutiny. Indeed, the Supreme Court itself has held "that […] physical intrusion, penetrating beneath the skin, infringes an expectation of privacy that society is prepared to recognize as reasonable."[21]

But DNA sampling methods have evolved. Nowadays, it is more common to extract DNA by applying a sticky patch to the skin on an individual's forearm for a moment to acquire epidermal cells without puncturing the skin surface.[22] There is no sub-dermal physical intrusion. The invasion of personal space required is minimal. The patch is applied and removed in a matter of seconds. Courts would likely find that such a negligible intrusion does not violate reasonable societal expectations of privacy. The cell extraction procedure would therefore not constitute a search, and the provisions of the 4th Amendment would not be called into play.[23]

If the DNA sampling process is held to constitute a search, would it violate the Fourth Amendment?

Even if the extraction and storage of DNA information necessary for the identification system is held to constitute a search under the Fourth Amendment, the process may still be found to be constitutional.

---

[20] *See id.*; *see also In re* Nontestimonial Identification Order Directed to R.H., 762 A.2d 1239, 1244 (Vt. 2000).
[21] *Skinner*, 489 U.S. at 616.
[22] *See* Kaye, Smith and Imwinkelried, *supra* note 7.
[23] Rothstein, *supra* note 15, at 134-35.

The Fourth Amendment requires that searches and seizures be reasonable. A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing.[24] "[H]owever, […] a showing of individualized suspicion is not a constitutional floor, below which a search must be presumed unreasonable."[25] "[W]here a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context" and thus whether the search is unreasonable.[26]

The DNA identification card scheme at issue here would require suspicionless searches if it is to be applied to a large portion of the population.[27] Therefore, in order to be reasonable, in compliance with the provisions of the 4th Amendment, the search must first be proven to respond to special governmental needs, beyond the purposes of law enforcement, and secondly, the government's interest in the search must be shown to outweigh the individuals' privacy interests.

1. Special needs

The U.S. has a special need for the DNA identification system at issue here, and the searches that go hand in hand with it. September 11th highlighted how vulnerable the country is to attack, even from within. The demonstrated ability of its opponents to effortlessly infiltrate American society before striking has prompted the Bush Administration to declare a more or less permanent state of alert. But the danger is not limited to foreign nationals. Terrorist organizations can no doubt count a number of American citizens in their ranks. John Walker Lindh and Richard Reid are only two of the most recent examples of citizens of Western countries choosing to fight against the interests of their homeland.

At times like these, it is therefore crucial not only for the law enforcement authorities and the government, but also for private entities such as commercial airlines, public transport companies, weapons retailers, and others, to be able to accurately identify all individuals. In the

---

[24] *See* Chandler v. Miller, 520 U.S. 305, 308 (1997).

[25] *Skinner,* 489 U.S. at 624 (drug and alcohol tests for railway employees involved in train accidents or found to be in violation of particular safety regulations); s*ee* Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (random drug testing of student-athletes); *see also* National Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989) (drug tests for United States Customs Service employees seeking transfer or promotion to certain positions).

[26] *Von Raab*, 489 U.S. at 665-66.

[27] Richard Sobel, *The Demeaning of Identity and Personhood in National Identification*, 15 HARV. J.L. & TECH. 319, 341 (2002); Baechtel, *supra* note 18, at 407 (applying biometric identification scheme to people entering the country); Richard Sobel, The *Degradation of Political Identity under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 46 (2002) (applying DNA scheme to newborns).

past, the Supreme Court has held the need to ensure the sobriety of railroad conductors[28], and the need for Customs officers to be drug-free[29], to constitute special governmental needs. The present need for foolproof identification and the increased level of national security it entails, would no doubt qualify as one too.

Admittedly, the scheme proposed here would not completely shield the country from the threat of terrorism.[30] Foreign nationals, or people with no hint of a shady past would not be hindered by the card system. But the DNA identification card would help in many other ways: it would make it more difficult for the same individual to strike twice, and would make it considerably more difficult for terrorists to assume false identities.[31] The database would also provide a potential stepping stone towards a greater goal: an international database, allowing the identification of all foreign nationals with the help of similar databases abroad.

In the meantime, a national DNA database is the best option available. There might never be complete protection against the threat of terrorism. But in these times of war, every little bit of protection helps.

2. Non law-enforcement purposes

The second point to be considered, when analyzing the special needs exception to the probable cause or warrant requirement, is whether the search is conducted for non-law enforcement purposes. If a search's immediate goal is to generate evidence for law enforcement purposes, courts may not allow state authorities to dispense with the need for a warrant or probable cause before conducting the search.[32]

If, however, courts find that the "special need" advanced as justification for the absence of individualized suspicion is "one divorced from the State's general law enforcement interest"[33], the search may still be found to be constitutional.[34] "[T]he presence of a law enforcement purpose does not [however] render the special needs doctrine inapplicable."[35] All that is required is that law enforcement not be the primary purpose of the intrusion into the individual's privacy.[36]

In the case at issue, the DNA identification scheme would not be intended primarily for law enforcement use. It is undeniable that the card could prove useful to law enforcement

---

[28] *Skinner*, 489 U.S. at 602.
[29] *Von Raab*, 489 U.S. at 679.
[30] Sobel, 15 HARV. J.L. & TECH. 319, *supra* note 26, at 367.
[31] *Id.* at 327.
[32] *See* Ferguson v. City of Charleston, 532 U.S. 67 (2001).
[33] *Id*. at 79.
[34] *See id*.
[35] *Id.* at 101 (Scalia, J., dissenting).
[36] Rothstein, *supra* note 9, at 154-55.

authorities in the performance of their duties, but that is not in and of itself sufficient to render the search unconstitutional. Greatest use for the card would in all likelihood be found as an identification tool in non-law enforcement settings such as ID checks at airport check-in desks, for example, or as a replacement for the social security card.

3. Balancing test

Once it has been settled that there is a special need for the intrusion, and that the purpose behind the intrusion goes beyond mere law enforcement, the balancing test cited in *Von Raab* is to be applied. The reasonableness of the search is to be determined by a careful balancing of governmental and private interests.[37] The Court would have to take into consideration a host of factors when applying this test.

First, the U.S. has a substantial interest in preventing the occurrence on its soil of any further terrorist attacks. The proportions of the harm to be avoided would weigh strongly in favor of the implementation of the card scheme.

Second, the Court should consider whether the purpose of the DNA extraction and isolation is clear, and whether there are "protections against the dissemination of the information to third parties."[38] If there is a clear purpose to the DNA extraction, and measures are taken to avoid the risk of the information thus gleaned from being disseminated, the intrusion on the individual's privacy interests is more likely to be deemed minor. In the present case, the purpose of the sampling is clear: to provide the country with a foolproof identification system. With regards to protections against dissemination, a system wherein all the DNA information would only be available to trustworthy medical personnel is easily imaginable.[39] Such a system might allow law enforcement officers only to have access to the results of identification tests, not the actual information contained on the cards, for example.[40]

Third, when evaluating the individual's privacy interests, it is crucial for the Court to consider the extent of the physical intrusion required, and the nature of the information gleaned as a result of the infringement on the individual's privacy. As discussed above, it is most likely that new methods in DNA extraction technology would limit the intrusion into any individual's privacy to a bare minimum. Furthermore, the information gleaned would most likely consist of non-coding tracts of DNA, that is, sequences that are not translated into proteins.[41] There would

---

[37] *Von Raab*, 489 U.S. at 665-66.
[38] *See Ferguson*, 532 U.S. at 78.
[39] Kaye, *supra* note 7, at 7.
[40] *See* Sonia Arrison & Solveig Singleton, *Will the Government's Use of Biometrics Endanger American Civil Liberties?*, WASHINGTON TIMES, Feb. 25, 2002, available at 2002 WL 8338249.
[41] Kaye, Smith and Imwinkelried, *supra* note 7, at 6; *see also* Rothstein, *supra* note 9, at 162.

thus only be a very minimal invasion of the individual's privacy, as no real information other than that needed for identification purposes could be obtained from the test results.

Finally, the Court would have to consider how long the DNA information of each individual was to be retained by the authorities after extraction. The longer the samples are kept, the more likely they are to be misused by the authorities, either to reveal future health risks, or to be disclosed to third parties such as insurers and employers.

Conclusion

Taking all these factors into consideration, the Court would then have to apply the *Von Raab* balancing test. The weight to be attributed by the Court to each one of the factors discussed above is difficult to predict at this point, because the "special need" at issue here is out of proportion with any encountered by the Court in the past, and because the modalities of the scheme have yet to be determined. But a holding that such a DNA card scheme complies with the 4th Amendment is not beyond the realm of imagination. We might scoff at the possibility of such a DNA card ever being introduced in our lifetimes, and may feel protected by the 4th Amendment, but this is not a clear cut issue. September 11th may have touched our lives in more ways than we know.

By: Ben Quarmby