T E S T I M O N Y

RAND

Biometrics: Facing Up to Terrorism

John D. Woodward, Jr.

CT-191

December 2001

Written testimony presented to the Senate Judiciary Committee's subcommittee on Technology, Terrorism and Government Information on November 14, 2001

This testimony is based on a variety of sources, including research conducted at RAND. However, the opinions and conclusions expressed are those of the author and should not be interpreted as representing those of RAND or any of the agencies of others sponsoring its research. This written testimony was submitted by John D. Woodward, Jr., a senior policy analyst at RAND, to the Senate Judiciary Committee's Subcommittee on Technology, Terrorism, and Government Information for its hearing on "Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism," held in Washington, D.C. on November 14, 2001.

For more information on RAND Arroyo Center, contact the Director of Operations (telephone 310-393-0411. Extension 6500; FAX 310-451-6952; e-mail donnab@rand.org), or visit the Arroyo Center's Web site at http://www.rand.org/organization/ard/.

Published 2001 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, Virginia 22202-5050
201 North Craig Street, Suite 102, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information,
contact RAND Distribution Services: Telephone: 310-451-7002;
Fax: 310-451-6915; or Email: order@rand.org

As the nation recovers from the attacks of September 11, 2001, we must rededicate our efforts to prevent any such terrorist acts in the future. Although terrorism can never be completely eliminated, we, as a nation, can take additional steps to counter it. We must explore many options in this endeavor. Among them, we should examine the use of emerging biometric technologies that can help improve public safety. While there is no easy, foolproof technical fix to counter terrorism, the use of biometric technologies might help make America a safer place.

"Biometrics" refers to the use of a person's physical characteristics or personal traits to identify, or verify the claimed identity of, that individual. Fingerprints, faces, voices, and handwritten signatures are all examples of characteristics that have been used to identify us in this way. Biometric-based systems provide automatic, nearly instantaneous identification of a person by converting the biometric—a fingerprint, for example—into digital form and then comparing it against a computerized database. In this way, fingerprints, faces, voices, iris and retinal images of the eye, hand geometry, and signature dynamics can now be used to identify us, or to authenticate our claimed identity, quickly and accurately. These biometric technologies may seem exotic, but their use is becoming increasingly common. In January 2000, *MIT Technology Review* named biometrics as one of the "top ten emerging technologies that will change the

John Woodward, Jr., a former CIA operations officer, is a senior policy analyst at RAND. He thanks Jon Grossman, Peter Higgins, Bob Preston, Jack Riley, and Shirley Woodward for their helpful comments. Research assistant Christopher Horn provided excellent suggestions and support. The views represented in this issue paper are the author's own.

world." And after September 11th, biometric technologies may prove to be one of the emerging technologies that will help safeguard the nation.

This issue paper does not advance the argument that biometrics would have prevented the September 11th attacks. Nor does it present biometrics as a complete solution to the terrorist problem. Rather, it offers recommendations as to how biometric technologies can be used to improve security and thereby help safeguard our communities against future terrorist attacks. Specifically, this issue paper discusses how biometric technologies could be used to impede terrorism in three critical areas:

1. Controlling access to sensitive facilities at airports,
2. Preventing identity theft and fraud in the use of travel documents, and
3. Identifying known or suspected terrorists.

It further offers a proposed counterterrorist application that uses a type of biometric known as facial recognition to identify terrorists.

Controlling Access

Sensitive areas of the nation's ports of entry, particularly airport facilities, need to be safeguarded so that only authorized personnel can gain access to them. Accordingly, individuals who have authorized access to sensitive areas of airport facilities must be identified and distinguished, accurately and efficiently, from those who do not. Currently, badges and tokens such as keys or passcards are used to identify authorized personnel and to control access to these areas. For example, display of a photograph identification badge may be all that is needed to gain access to some

employee-only areas of an airport. Similarly, individuals with authorized access to a particular area in an airport may use a magnetic strip badge or card which, when swiped through a reader, allows access to baggage loading areas, runways, and aircraft. Such access control measures, based on items in an individual's physical possession, are not particularly secure. The system assumes that whoever possesses the badge or the passcard is the person who should be granted access, when in reality, badges and tokens are easily forged, stolen, or misplaced.

Combining something a person must physically *possess* with something a person must *know*, such as a password or personal identification number (PIN), improves security. For example, a system similar to an automated teller machine (ATM), which requires both a magnetic strip card and a PIN, can reduce the threat to security from lost or stolen cards. The system is still easily compromised, however: given the profusion of PINs and passwords and our difficulty in remembering them, their owners often write them on the card itself or on a piece of paper stored nearby.

Access control to sensitive facilities can be improved by using biometric-based identifiers. In other words, instead of identifying an individual based on something he has (a badge), or something he knows (a password or a PIN), that person will be identified based on something he *is*. For example, instead of flashing a badge, an airline worker with a need to access sensitive areas of airports could be required to present a biometric, say his iris, to a sensor. From a foot away and in a matter of seconds, this device captures the person's iris image, converts it to a *template*, or computer-readable representation, and searches a database containing the templates of

authorized personnel for a match. A match confirms that the person seeking access to a particular area is in fact authorized to do so. This scenario is not science fiction. Such a system has been used at Charlotte-Douglas International Airport in North Carolina.

While not foolproof, such a biometric system is much harder to compromise than systems using a badge or badge plus PIN. As such, a biometric system to authenticate the identity of individuals seeking access to sensitive areas within airports or similar facilities represents a significant increase in security. And to the extent that terrorist acts can be thwarted by the ability to keep unauthorized individuals out of these sensitive areas, this improvement in physical security could contribute directly to a decrease in the terrorist threat.

Preventing Immigration Fraud/Identity Theft

In addition to failures to authenticate the identity of airport employees, failures to accurately identify individuals as they cross through our borders can also contribute to a terrorist attack. It is important to ensure that necessary travel documents are used only by the person to whom they were issued. Like badges and tokens, passports, visas, and boarding passes can be forged, misplaced, or stolen. While anti-fraud measures are built into the issuance of such documents, there is room for improvement. A biometric template of, for example, one's fingerprint (or other biometric) could be attached to the document on a bar code, chip, or magnetic strip, making it more difficult for someone to adopt a false identity or forge a travel document. To ensure security, the biometric

should be encrypted and inserted into the document by a digital signature process using a trusted agent, such as a U.S. embassy's visa section.

In addition to helping prevent fraud or identity theft, we can use biometrics to make it easier for certain qualified travelers to identify themselves. For example, the Immigration and Naturalization Service (INS) currently uses biometrics in the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS). Under INSPASS, over 45,000 international travelers, whose identities and travel papers have been vetted, have voluntarily enrolled in a system that verifies their identity at ports of entry using the biometric of hand geometry. By allowing these frequent travelers to pass through immigration quickly, INSPASS enables INS officers to devote more time and attention to problem cases.[1]

Identifying Known or Suspected Terrorists

As the criminal investigation of the September 11th attacks appears to demonstrate, some of the terrorists were able to enter the United States using valid travel documents under their true identities, passing with little difficulty through immigration procedures at U.S. ports of entry. Once in the country, they patiently continued their planning, preparation, training, and related operational work for months and in some cases years until that fateful day. Once inside the United States, the terrorists cleverly took advantage of American freedoms to help carry out their attacks.

According to media reports, however, at least three of the suicide attackers were known to U.S. authorities as suspected terrorists. In late August 2001, the

Central Intelligence Agency (CIA) passed information to the INS to be on the lookout for two men suspected of involvement in terrorist activities. The CIA apparently obtained videotape showing the men, Khalid Almihdhar and Nawaf Alhazmi, talking to people implicated in the *U.S.S. Cole* bombing. The videotape was taken in Kuala Lumpur, Malaysia, in January 2000. It is not clear when the CIA received it.

When the INS checked its database, it found that a Almihdhar and Alhazmi had successfully passed through INS procedures and had already entered the United States. The CIA asked the Federal Bureau of Investigation (FBI) to find them. But with both men already in the United States, the FBI was looking for two needles in a haystack. The FBI was still seeking the two when the hijackers struck. Khalid Almihdhar and Nawaf Alhazmi are believed to have been hijackers on American Airlines flight 77, which crashed into the Pentagon.

As the above details illustrate, we need a better way to identify individuals whom we know or suspect to be terrorists when they attempt to enter the United States. The use of biometric facial recognition is one way to make such identifications, particularly when U.S. authorities already have a photograph of the suspected terrorist whom they seek.

FaceCheck

Biometric facial recognition systems could be immediately deployed to help thwart future terrorist acts. Such a "FaceCheck" system, the term I use for the specific counterterrorism application discussed in this paper, can be done in a way that uses public safety resources effectively and efficiently and minimizes

inconvenience and intrusiveness for the average traveler.

In general, facial recognition systems use a camera to capture an image of a person's face as a digital photograph. In the most common form of facial recognition, this image is manipulated and reduced to a series of numbers that represent the image in relation to the "average" face. These numbers are often referred to as a template, which is then instantly searched against a "watchlist," or computerized database of suspected terrorists' templates. This search seeks to answer the question, "Is this person in the watchlist database?" A computer-generated match or "hit" alerts the authorities to the presence of a potential threat. The value of such a system in helping to prevent individuals such as Khalid Almihdhar and Nawaf Alhazmi from entering the country is clear. Indeed, according to the *Washington Post*, a government committee appointed by Secretary of Transportation Norman Y. Mineta to review airport security measures will recommend that facial recognition systems be deployed in specified airports to improve security.[2]

Operational Framework

Controlling access to sensitive facilities, as well as preventing immigration fraud and identity theft, can be accomplished with a variety of biometric systems. Such systems can accommodate users and are relatively easy to incorporate into current security systems (i.e., adding a digitally signed, encrypted biometric bar code to existing travel documents or badges). Moreover, the technology is readily available.

Identifying known or suspected terrorists presents

a greater challenge. While fingerprint and other biometric systems could be used to identify these individuals, government authorities might find it difficult to collect the fingerprints or iris scans of suspected terrorists in order to build the database against which to compare an unknown individual. Facial recognition biometric systems, however, offer a way around this problem. Specifically, facial recognition systems will allow the identification of a suspected or known terrorist even if the only identifying information we have is a photograph.

But the technology is not perfect, and it has yet to be fully vetted in real-world, operational settings.[3] Facial recognition systems received much public attention in January 2001 when authorities in Tampa, Florida deployed one at Super Bowl XXXV in an attempt to identify threats to public safety. At Raymond James Stadium, surveillance cameras scanned the crowd and captured images of spectators attending the Super Bowl. Authorities reported that the system made nineteen computer matches. Based on this limited experience, it is difficult to discern how well the system worked. The police did not make any arrests based on the computer matches, and it is therefore not known whether any of these matches were "false matches," also known as "false positives," i.e., false alarms because the individual was not in fact the person the system thought he was. In other words, although the computer may indicate a match, this information is not confirmed until the police arrive on the scene and scrutinize the suspect.

Dr. James L. Wayman of San Jose State University, a leading biometrics expert, has explained that although human beings generally can perform facial recognition processes with relatively high fidelity and

at long distances, these activities are still very challenging for technological systems. At the most basic level, even detecting whether a face is present in a given electronic photograph is a difficult technical problem. Dr. Wayman has noted that unless the photograph is captured under very controlled conditions, ideally with each subject looking directly into the camera and filling the area of the photo completely, the system may have difficulty identifying the individual or even detecting his face in the photograph.

Recent technical analyses of facial recognition systems indicate that while the technology shows promise, it is not yet advanced enough to be considered fully mature. The "Facial Recognition Vendor Test 2000" study makes clear that the technology is not yet perfected.[4] This comprehensive study of current facial recognition technologies, sponsored by the Department of Defense (DoD) Counterdrug Technology Development Program Office, the Defense Advanced Research Projects Agency (DARPA), and the National Institute of Justice, showed that environmental factors such as differences in camera angle, direction of lighting, facial expression, and other parameters can have significant effects on the ability of systems to recognize individuals.

Recent tests of these technologies indicate that the current capabilities of facial recognition systems are limited. For example, Professor Takeo Kanade of Carnegie-Mellon University is skeptical of the system's reliability in "a typical airport situation." Dr. Wayman has stressed that there is a great deal of room for improvement in both the algorithms used to match sampled faces and in databases of file images.

The moderate level of success that current systems have displayed must be placed in the appropriate context, however; while human beings can often readily recognize faces at long distances, the efficiency of such recognition falls precipitously when posted human guards are asked to scrutinize large crowds in search of small numbers of potentially threatening individuals. As a result, for these tasks, the current technical capabilities may still exceed more traditional approaches, and combinations of automated and human-based recognition could be advantageous. To assist in this determination, there is definite need for independent organizations to test, assess, and validate the various biometric technologies.

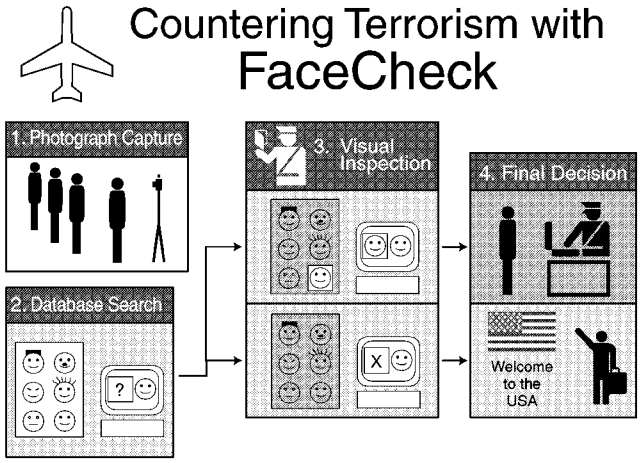
It is of critical importance that the capabilities of systems and potential ways of applying those capabilities are appropriately matched to security and surveillance needs so that individuals expect neither too much nor too little from these emerging technological tools.

Although facial recognition is not a perfect technology, we should not let the perfect become the enemy of the good. The overall challenge is to make it better. Fortunately, gifted scientists and engineers are working on this challenge, and in light of the September 11th attacks, the government is likely to make additional resources available to encourage research, development, testing, and evaluation. In the meantime, we can use facial recognition operationally in a way that minimizes its weaknesses. The system works best when environmental factors such as camera angle, lighting, and facial expression are controlled to the maximum extent possible. We must apply this lesson to our operational framework.

If a person (including a terrorist) is coming to the United States from overseas, he must pass through an

immigration checkpoint at the port of entry. At this checkpoint, the INS official scrutinizes the person, asks questions, and inspects the person's travel documents. The official then makes a decision as to whether the person gets into the box, i.e., enters the United States. This immigration checkpoint is one of the nation's vital first lines of defense against terrorist entry. From the perspective of counterterrorism, this checkpoint is a chokepoint where the would-be terrorist is at his most vulnerable. This is the first and probably only place in the United States where he will be closely scrutinized by trained federal officials. Here is how FaceCheck can make the checkpoint a more formidable bastion.

An individual processing through an immigration checkpoint at a port of entry should be subject to a FaceCheck whereby he would be required as part of immigration processing to pose for a photograph under completely controlled conditions. This way we minimize facial recognition's technological imperfections, which derive in large measure from attempting



to use the system to find a face in a crowd. The photograph would then be processed by the facial recognition system and run against a watchlist database of suspect terrorists. If the system indicates a match, this result would be confirmed by visual inspection by the authorities, and the person could be taken to a secondary interview for heightened scrutiny.

Facial recognition systems do not necessarily have to be implemented to process every individual seeking to enter the United States. Rather, the authorities should use FaceCheck in a more strategic way. This would include using it randomly; in targeted ways; and in conjunction with other information. For example, FaceCheck could be run on every so many people from a given flight. It could be used at different ports of entry at different times and for different flights. Similarly, FaceCheck teams could deploy to specific ports of entry at specific times to target a specific flight in light of threat information. Testers—human guinea pigs whose images have been entered into the watchlist database—should be included in the immigration processing to rigorously evaluate the system: How well did FaceCheck do in identifying suspects?[5]

Moreover, while we do not have to use the system on all passengers entering the United States, we should consider setting up FaceCheck stations at ports of entry and have passengers pose for photographs as though the system were in continuous use. In this way, we keep terrorists guessing as to where the systems are actually deployed or in use. We should also experiment with FaceCheck systems using closed-circuit surveillance cameras to capture images clandestinely at certain ports of entry. In this way, we can learn how well such systems work in

realistic operational environments and gain information to improve their technical capabilities. Again, we do not need to inform passengers as to where such systems are actually deployed.

We also need to consider using FaceCheck for visa processing at our embassies and consulates overseas. We could easily require a visa applicant to submit to a photograph taken under controlled conditions. We could then run a search against the watchlist database. Similarly, we do not need to inform visa applicants overseas whether we are actually running FaceCheck.[6]

Dedicated, highly trained terrorists may be able to defeat facial recognition systems. One technique may be for a terrorist to undergo cosmetic surgery to alter his facial features. As a result, he will not match his database photograph. Similarly, terrorists may try to enter the United States illegally by crossing the relatively porous borders with Canada and Mexico. But although facial recognition systems might be defeated by a surgeon's skill or an illegal border crossing, at least we force terrorists to take additional steps that drain their resources and keep them on the defensive.[7]

Policy Issues

Though these facial recognition systems are not technically perfected, they are improving. There is little reason to doubt that as the technology improves, it will eventually be able to identify faces in a crowd as effectively as it currently identifies a face scanned under controlled circumstances. And while civil libertarians might decry the use of this technology as an invasion of privacy, the key lies in balancing the need

for security with the need to protect civil liberties.[8] In this regard, three brief points need to be made.

First, we do not have a constitutional right to privacy in the face we show in public. The United States Supreme Court has determined that government action constitutes a "search" when it invades a person's reasonable expectation of privacy. But the Court has found that a person does not have a reasonable expectation of privacy in those physical characteristics that are constantly exposed to the public, such as one's facial features, voice, and handwriting. Therefore, although the Fourth Amendment requires that a search conducted by government actors be "reasonable," which generally means that the individual is under suspicion, the use of facial recognition does not constitute a search. As a result, the government is not constrained, on Fourth Amendment grounds, from employing facial recognition systems in public spaces. Although the use of facial recognition may generate discussion of the desirability of enacting new regulations for the use of the technology, such use is allowed under our current legal framework.

Secondly, current legal standards recognize that we are all subject to heightened scrutiny at our borders and ports of entry. The "border exception" to the Fourth Amendment recognizes the "the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."[9] Accordingly, such searches are reasonable and do not require a warrant, probable cause, or even reasonable suspicion. When we transit our borders, therefore, the authorities can closely scrutinize our person and property in ways that they could not do in another setting. Even within our own borders, the

law requires airport facilities to conduct security screening of passengers' persons and personal effects, and it is unlawful even to make jokes about threats on airport property.

Finally, it is worth noting that facial recognition systems are not relied upon to make final determinations of a person's identity. Rather, the system alerts the authorities so that additional screening and investigation can take place. And though the system will make false matches that will subject innocent passengers to additional questioning and scrutiny, the current system routinely does the same.

Existing Government Resources

There are many existing resources in this field that can aid in the implementation of biometric technology for the uses described above. Since 1992, the National Institute of Standards and Technologies (NIST), the national security community, and other federal agencies have participated in the Biometric Consortium (BC), which serves as the U.S. government's focal point for biometric technologies. However, the BC currently operates on a very lean budget with limited staff.

The Department of Defense is also involved in exploring the uses of biometric technology. In the wake of the Khobar Towers terrorist attack in Saudi Arabia in 1996, DARPA embarked on a $50 million initiative known as "Human ID at a Distance," a major component of which is facial recognition. DARPA's ambitious goal is to help develop biometric technologies, like facial recognition, that can be deployed to identify a known terrorist at some distance, before he closes on his target.

The nation's political leadership has also recognized the potential of biometric technologies. As part of an appropriations bill for 2001, Congress addressed the use of biometrics technology for DoD to use in its information assurance programs. Specifically, Public Law 106-246, which was signed into law on July 13, 2000, included a provision making the Army "the Executive Agent to lead, consolidate, and coordinate all biometrics information assurance programs of the Department of Defense." Soon thereafter, Pentagon leadership created a Biometrics Management Office to consolidate oversight and management of biometric technology for DoD.

Policy Recommendations

The U.S. government has taken positive steps to encourage the use of biometrics. It is time to do more. The newly established Office of Homeland Security (OHS) is a logical place to coordinate these efforts. Specifically, OHS can focus part of its efforts on using biometrics to counter terrorism. As a first step, OHS, working with other concerned agencies like the Department of Justice, INS, FBI, CIA, Department of State, and Department of Transportation, should draft guidelines to explain how biometric technologies, particularly the FaceCheck system, should be used and implemented. This OHS coordination effort is essential for any biometrics that would be used in conjunction with travel documents where interoperability and technical standards are of critical importance.

These guidelines should also address a crucial aspect of any FaceCheck system—the data that are

included in the watchlist database. In this regard, the guidelines must include rigorous technical and procedural controls on the information that goes into the watchlist database. The nation's focus now is on the war against terrorism; the focus of the watchlist database should similarly be on locating known or suspected terrorists and deterring unknown terrorists from entering the United States. Depending on resources and constraints, the watchlist might also include certain individuals for whom there are felony arrest warrants outstanding.

Accordingly, OHS should immediately task the law enforcement and intelligence communities to provide photographs of known and suspected terrorists for the watchlist database. The security and intelligence services of foreign states could also contribute to this effort. It would also seem advisable to expand FaceCheck so that it can be used among other nations at their ports of entry to help identify terrorists around the globe.

With an eye toward the future, OHS should work closely with the BC, INS, and DoD's ongoing biometric initiatives to encourage the U.S. government's biometric development efforts. Priority should be placed on rigorous independent vetting and testing of biometric technologies.

Conclusion

There is no high-tech silver bullet to solve the problem of terrorism. And it is doubtful that facial recognition or other biometric technologies could have prevented the terrorist attacks on September 11th. But to the extent we can improve access control at sensitive facilities such as airports, reduce identity

theft and immigration fraud, and identify known or suspected terrorists, then we make terrorism more difficult in the future. Biometrics is one technology that can help us achieve the goal of a safer America.

NOTES

[1]To learn more about INSPASS, visit *http://www.ins.gov/graphics/lawenfor/bmgmt/inspect/inspass.htm.*

[2]On September 24, 2001, Visionics Corporation, a company specializing in biometric products, issued a white paper, "Protecting Civilization from the Faces of Terror: A Primer on the Role Facial Recognition Technology Can Play in Enhancing Airport Security." Joseph Atick, the CEO of Visionics, testified before the government committee. For additional information, see *www.visionics.com.* Similarly, Viisage Technology Inc. has been selected to install its facial recognition system at a U.S. airport. This deployment is believed to be the first-in-the-nation use of face-recognition technology for airport security. The system is expected to be operational in 2001. For further details, see Viisage Press Release, "Viisage Selected to Deploy the First Face-Recognition Technology System for Security in a U.S. Airport," October 4, 2001, available at *http://www.viisage.com.*

[3]See, e.g., Lee Gomes, "Can Facial Recognition Help Snag Terrorists?" *Wall Street Journal,* September 27, 2001, p. B11.

[4]The "Facial Recognition Vendor Test 2000" study is available at *http://www.dodcounterdrug.com/facialrecognition/FRVT2000/frvt2000.htm.*

Other large-scale evaluations include the report of the United Kingdom's Communications-Electronics Security Group (CESG) Biometrics Working Group (BWG), "Biometric Test Programme Report," available at *http://www.cesg.gov.uk/technology/biometrics/,* and the Facial Recognition Technology (FERET) program's evaluation of algorithms, available at *http://www.dodcounterdrug.com/facialrecognition/FERET.feret.htm.*

The Visionics white paper cited above does not discuss test and evaluation issues related to the use of facial recognition technology.

[5]An abundant source of volunteer testers could include aircrews, for example.

[6]Along these lines, Congress is considering requiring foreigners to have identification cards bearing their digitized fingerprints for entry into the United States. The legislation's goal is to permit greater screening of foreign visitors.

[7]Through coordinated efforts with our neighbors, it might be possible that Canada and Mexico would embrace deployment of a FaceCheck system.

[8]For a more detailed discussion of the policy concerns attached to facial recognition, see, e.g., John D. Woodward, Jr., *Super Bowl Surveillance: Facing Up to Biometrics,* Santa Monica, CA: RAND, IP-209, 2001.

[9]*United States* v. *Ramsey*, 431 U.S. 606, 616 (1977).