Testimony of

James Dempsey

November 18, 2003

Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology

before the
Senate Committee on the Judiciary

"America after 9/11: Freedom Preserved or Freedom Lost?"

November 18, 2003

Mr. Chairman, Sen. Leahy, Members of the Committee, thank you for the opportunity to testify today at this important set of oversight hearings on the nation's responses to terrorism and the impact on civil liberties. Since 9/11, the federal government has engaged in serious abuses of constitutional and human rights. The most egregious of these abuses have taken place outside of the PATRIOT Act or any other Congressional authorization. In the PATRIOT Act itself, not surprisingly given the pressures under which that law was enacted, the pendulum swung too far, and Congress eliminated crucial checks and balances that should now be restored in the interest of both freedom and security.

Terrorism poses a grave and imminent threat to our nation. The government must have strong legal authorities to prevent terrorism to the greatest extent possible and to punish it when it occurs. These authorities must include the ability to conduct electronic surveillance, carry out searches effectively, and obtain business records pertaining to suspected terrorists. These powers, however, must be guided by the particularized suspicion principle of the Fourth Amendment, and subject to Executive, legislative and judicial controls as well as a measure of public oversight.

During consideration of the PATRIOT Act and today, the debate has never been about whether the government should have certain powers. Instead, the focus of concern has always been on what standards those powers should be subject to. Of course, the FBI should be able to carry out roving taps during intelligence investigations of terrorism, just as it has long been able to do in criminal investigations of terrorism. But the PATRIOT Act standard for roving taps in intelligence cases lacks important procedural protections applicable in criminal cases. Of course, the law should clearly allow the government to intercept transactional data about Internet communications (something the government was doing before the PATRIOT Act anyhow). But the pen register/trap and trace standard for both Internet communications and telephones is so low that judges are reduced to mere rubber stamps, with no authority to even consider the factual basis for a surveillance application. Of course, prosecutors should be allowed to use FISA evidence in criminal cases (they did so on many occasions before the PATRIOT Act) and to coordinate intelligence and criminal investigations (there was no legal bar to doing so before the PATRIOT Act). But prosecutors should not be able to initiate and control FISA investigations, and FISA evidence in criminal cases should not be shielded from the adversarial process (as it has been in every case to date).

Prior to 9/11, the government had awesome powers, but failed to use them well. Those failures had little if anything to do with the rules protecting privacy or due process, but the Executive Branch has proceeded since 9/11 as if the elimination of checks and balances would make its efforts more effective. The lessons of history and the experience of the past two years show that law enforcement and intelligence agencies without clear standards to guide them and without oversight and accountability are more likely to engage in unfocused, unproductive activity and more likely to make mistakes in ways that are harmful to civil liberties and ineffective, even counterproductive from a security standpoint.

The promised trade-off between freedom and security is often a false one. There are undoubtedly people in the United States today planning additional terrorist attacks, perhaps involving biological, chemical or

nuclear materials. Yet it is precisely because the risk is so high that we need to preserve the fullest range of due process and accountability in the exercise of government powers.

Abuses of Civil Liberties and Human Rights Since 9/11 Outside the PATRIOT Act

The phrase "the PATRIOT Act" has become a symbol or a shorthand reference to the government's response to terrorism since 9/11. Both the Justice Department and its critics, abetted by the media, share responsibility for this. The PATRIOT Act ends up being cited for things that are not in it. Both sides in the debate have claimed that the PATRIOT Act is more important than it is. Certainly, many of the worst civil liberties abuses since 9/11 have occurred outside the PATRIOT Act. These will be described in greater depth by others at this hearing and in other hearings the Committee will hold. But it is useful to outline them:

-- The detention of US citizens in military jails without criminal charges

For many Americans, it is simply inconceivable that a U.S. citizen could be held without criminal charges in a military prison. Yet that is precisely the situation today of two U.S. citizens. One of these, Jose Padilla, was arrested at Chicago's O'Hare airport by the FBI. He was transported to New York on a material witness warrant in connection with a criminal investigation. The President then plucked Padilla out the criminal justice system, turned him over to the military, and now claims the right to hold him indefinitely in military prison without criminal charges. This has to be a fundamental violation of the Constitution. Nothing in Ex parte Quirin, 317 U.S. 1 (1942) supports this. In Ex parte Quirin, the German saboteurs, including one who might have been a citizen, admitted that they were members of the official armed force of a nation with which the United States was in a declared war. Congress had authorized the use of military commissions to try violations of the law of war. None of these factors apply today.

-- The detention of foreign nationals in Guantanamo and other locations, with no due process and purportedly outside of any US or international legal scheme.

Over the past century, one of the most important achievements of international law in general and human rights in specific has been the general diffusion and acceptance of the principle that there is no place and no person outside the law. The drawing of all governments into a web of international obligations and constraints - obligations that range from human rights to arms control -- was one of the cornerstones of the successful effort to break the Soviet Union. It was a basis for the invasion of Iraq. It remains an impetus for the ongoing struggle for religious freedom and other civil liberties in China. And yet the President of the United States claims to have a found in Guantanamo a place outside of any system of law other than the one that he dictates. The President claims that his actions there are outside the jurisdiction of the U.S. courts, outside, of course, the reach of Cuban courts, and outside the jurisdiction of any international entity. He claims that the people held there fall between the cracks legally - they are not prisoners of war subject to the Geneva Conventions and they are not criminals and that he has the sole power to decide their fate. Yet it is clear that not all the people who have been detained at Guantanamo were terrorists. The Executive Branch, on its own schedule and at its discretion, has already concluded that some of those detained at Guantanamo were not dangerous at all, for it has released them. It is logical to assume that other victims of mistake are still in custody. The U.S. government, after all, relied on bounty hunters in Afghanistan, who had been promised enough money to support an entire village if they turned in an al Qaeda or Taliban member. Was there ever a situation more deserving of independent fact-finding to root out mistakes and false accusations?

-- The rendition of detainees to other governments known to engage in torture

It has been widely alleged, and anonymously acknowledged, that the US government has turned over people it detains to other governments knowing or expecting that they will be tortured.

-- Post 9/11 detentions of foreign nationals in the U.S.

Others can comment in detail on the multiple abuses posed by the government's treatment of immigrants since 9/11. There have been many. More than 1,200 immigrants were detained in this country in the months after 9/11. The government refused to release their names. Many were held for days, weeks, or even longer without charges. The INS blocked access to lawyers and families. In all cases designated as related to the September 11 investigation, the Justice Department ordered a blanket closing of deportation hearings. It

adopted a policy of denying bail and gave INS attorneys unilateral authority to automatically stay any bond-release ruling of an immigration judge. The abuses of civil liberties were documented by the Department of Justice Inspector General in his report of June 2003. The Committee has held a hearing on that report. The OIG found in June 2003 that many of the detainees did not receive core due process protections. The OIG found that the "vast majority" were never accused of terrorism related offenses but only of civil violations of federal immigration law. Most significantly, the OIG found that, at the time of arrest, the link between many of the detainees and the attacks of 9/11 was "extremely attenuated." The OIG concluded that the designation of detainees as "of interest" to the September 11 investigation was made in an "indiscriminate and haphazard" manner. In other words, the national security justification for the blanket closure of deportation hearings and the withholding of the names of the detainees was not sound - an example of how abuses result from the exercise of power without independent scrutiny. More recently, on September 8, 2003, the OIG reported that the DHS and DOJ were taking steps to address many of the problems identified.

-- Detentions of citizens

It is clear that the detentions without normal due process also swept up U.S. citizens. Fathi Mustafa, a naturalized U.S. citizen and his son, a U.S. citizen by birth, were arrested September 15, 2001 at Bush Intercontinental Airport in Texas after returning from a trip to Mexico to purchase leather products for their dry-goods store. Both were charged in federal court with passport fraud, on the ground that the laminate on their passport appeared to be altered (it may have been worn). Fathi Mustafa was released from jail on September 26 on a $100,000 bond. His son Nacer, the native born citizen, was held for 67 days. Both were cleared of all charges.

-- Abuse of the material witness law

Under a law little known even by most lawyers prior to 9/11, the material witness law, the U.S. government has arrested aliens and citizens alike and held them in jail without charges. Yet according to new reports, many had not been called to testify before a grant jury after months of detention. Steve Fainaru and Margot William, "Material Witness Law Has Many in Limbo: Nearly Half Held in War on Terror Haven't Testified, " Washington Post, p. A1, November 4, 2002. The Justice Department has refused to disclose information about these cases, making it difficult to determine what is going on, but the practice surely stretches the material witness law far beyond its intended purpose of allowing the government to preserve a witness's testimony.

Abuses under the PATRIOT Act

-- Sneak and Peek Searches

It would astound most Americans that government agents could enter their homes while they are asleep or their places of business while they are away and carry out a secret search or seizure and not tell them until weeks or months later. That is what Section 213 of the PATRIOT Act authorizes. Moreover, it applies equally to all federal offenses, ranging from weapons of mass destruction investigations to student loan cases. In our opinion, one of the clearest abuses of the PATRIOT Act is the government's admitted use of Section 213 sneak and peek authority in non-violent cases having nothing to do with terrorism. These include, according the Justice Department's October 24, 2003 letter to Senator Stevens, an investigation of judicial corruption, where agents carried out a sneak and peek search of a judge's chambers, a fraudulent checks case, and a health care fraud investigation, which involved a sneak and peek of a home nursing care business.

Section 213 fails in its stated purpose of establishing a uniform statutory standard applicable to sneak and peek searches throughout the United States. For a number of years, under various vague standards, courts have allowed delayed notice or sneak and peek searches. Section 213 confuses the law in this already confused area. In the PATRIOT Act, Congress did not try to devise a standard suitable to breaking and entering into homes and offices for delayed notice searches. Instead, the PATRIOT Act merely incorporated by reference a definition of "adverse result" adopted in 1986 for completely unrelated purposes, concerning access to email stored on the computer of an ISP. Under that standard, not only can secret searches of homes and offices be allowed in cases that could result in endangering the life of a person or destruction of evidence, but also in any case that might involve "intimidation of potential

witnesses" or "seriously jeopardizing an investigation" or "unduly delaying a trial." These broad concepts offer little guidance to judges and will bring about no national uniformity in sneak and peek cases.
Section 213 also leaves judges guessing as to how long notice may be delayed. The Second and Ninth Circuits had adopted, as a basic presumption, a seven day rule for the initial delay. Section 213 says that notice may be delayed for "a reasonable period." Does this mean that courts in the Ninth Circuit and the Second Circuit no longer have to adhere to the seven day rule? At the least, it suggests that courts outside those Circuits could make up their own rule. "Reasonable period" affords judges considering sneak and peek sneak and peek searches no uniform standard.
But there is a deeper problem with Section 213: The sneak and peek cases rest on an interpretation of the Fourth Amendment that is no longer correct. The major Circuit Court opinions allowing sneak and peek searches date from the 1986, United States v. Freitas, 800 F.2d 1451 (9th Cir.), and 1990, United States v. Villegas, 899 F.2d 1324 (2d Cir.) before the Supreme Court decision in Wilson v. Arkansas, 514 U.S. 927 (1995). The sneak and peak cases were premised on the assumption that notice was not an element of the Fourth Amendment. United States v. Pangburn, 983 F.2d 449, 453 (2d Cir. 1993) starts its discussion of sneak and peek searches stating: "No provision specifically requiring notice of the execution of a search warrant is included in the Fourth Amendment." Pangburn goes on to states, "The Fourth Amendment does not deal with notice of any kind ... ." Id. at 455. United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000), even though it was decided after Wilson, states, "The Fourth Amendment does not mention notice." Yet in Wilson v. Arkansas, the Supreme Court, in a unanimous opinion by Justice Thomas, held that the knock and notice requirement of common law was incorporated in the Fourth Amendment as part of the constitutional inquiry into reasonableness, directly repudiating the reasoning of the sneak and peek cases. Wilson v. Arkansas makes it clear that a search without notice is not always unreasonable, but surely the case requires a different analysis of the issue than was given it by those courts that assumed that notice was not a part of the constitutional framework for searches. A much more carefully crafted set of standards for sneak and peek searches, including both stricter limits of the circumstances under which they can be approved and a seven day time limit, is called for. Even then, secret searches of homes must be on shaky constitutional ground except in investigations of the most serious crimes.

-- Section 215 - Business Records

Section 215 is not a matter of abuse, since the Justice Department recently admitted that it has never been used, but it does illustrate one of the fundamental flaws in Congress's approach to the PATRIOT Act in the frenzied and emotion-filled days after 9/11: there was never any discussion whether the new authorities were needed. Now, after two years of debate in which the Attorney General defended Section 215 as a key tool in the fight against terrorism, he has more recently announced that Section 215 has never been used even once, not only not for library records but also not for any other kind of business records.
Section 215 amended the Foreign Intelligence Surveillance Act to authorize the government to obtain a court order from the FISA court or designated magistrates to seize "any tangible things (including books, records, papers, documents, and other items)" that an FBI agent claims are "sought for" an authorized investigation "to protect against international terrorism or clandestine intelligence activities." The subject of the order need not be suspected of any involvement in terrorism whatsoever; indeed, if the statute is read literally, the order need not name any particular person but may encompass entire collections of data related to many individuals. The Justice Department often says that the order can be issued only after a court determines that the records being sought are "relevant" to a terrorism investigation. Actually, the section does not use the word "relevance." Relevance is quite broad but has some outer limits. The PATRIOT Act provision says only that the application must specify that the records concerned are "sought for" an authorized investigation. And the judge does not determine that the records are in fact "sought for" the investigation - the judge only can determine whether the FBI agent has said that they are sought for an investigation. The PATRIOT Act does not require that applications must be under oath. It doesn't even require that the application must be in writing. It doesn't require, as for example the pen register law does, that the application must indicate what agency is conducting the investigation. In Section 505 of the PATRIOT Act similarly expanded the government's power to obtain telephone and email transactional records, credit reports and financial data with the use of a document called the National Security Letter (NSL), which is issued by FBI officials without judicial approval.
The Justice Department argues that Section 215 merely gives to intelligence agents the same powers

available in criminal cases, since investigators in criminal cases can obtain anything with a subpoena issued on a relevance standard. First of all, as noted, the standard in Section 215 and two of the three NSL statutes is less than relevance. Second, a criminal case is at least cabined by the criminal code - something is relevant only if it relates to the commission of a crime. But on the intelligence side, the government need not be investigating crimes - at least for non-U.S. persons, it can investigate purely legal activities by those suspected of being agents of foreign powers.

There are other protections applicable to criminal subpoenas that are not available under Section 215 and the NSLs. For one, third party recipients of criminal subpoenas can notify the record subject, either immediately or after a required delay. Section 215 and the NSLs prohibit the recipient of a disclosure order from ever telling the record subject, which means that the person whose privacy has been invaded never has a chance to rectify any mistake or seek redress for any abuse. Secondly, the protections of the criminal justice system provide an opportunity for persons to assert their rights and protect their privacy, but those adversarial processes are not available in intelligence investigations that do not end up in criminal charges. Since Section 215 has never been used, it should be repealed as unnecessary. At the least, it should be amended to require a factual showing of particularized suspicion.

-- Use of FISA evidence in criminal cases without full due process

Before the PATRIOT Act, there was no legal barrier to using FISA information in criminal cases. The wall between prosecutors and intelligence officers as it evolved over the years was a secret invention of the FISA court, the Department's Office of Intelligence Policy and Review, and the FBI, with little basis in FISA itself. It did not serve either civil liberties or national security interests. The primary purpose standard did not have to be changed to promote coordination and information sharing.

As a result of the PATRIOT Act and the decision of the FISA Review Court, criminal investigators are now able to initiate and control FISA surveillances. The number of FISA has gone up dramatically. USA Today reported on November 11 that in the past year, the FISA court has granted about 2,000 requests by government agents to conduct electronic eavesdropping. In 2002, the court approved 1,228 requests. Toni Locy, "For linguists, job is patriotic duty, USA Today, November 11, 2003, http://www.usatoday.com/news/washington/2003-11-11-linguists_x.htm. The FISA court now issues more surveillance orders in national security cases than all the other federal judges issue in all other criminal cases. In the past, when FISA evidence has been introduced in criminal cases, it has not been subject to the normal adversarial process. Unlike ordinary criminal defendants in Title III cases, criminal defendants in FISA cases have not gotten access to the affidavit serving as the basis for the interception order. They have therefore been unable to meaningfully challenge the basis for the search. Defendants have also been constrained in getting access to any portions of the tapes other than those introduced against them or meeting the government's strict interpretation of what is exculpatory. This is an abuse. If FISA evidence is to be used more widely in criminal cases, and if criminal prosecutors are able to initiate and control surveillances using the FISA standard, then those surveillances should be subject to the normal criminal adversarial process. Congress should make the use of FISA evidence in criminal cases subject to the Classified Information Procedures Act. Congress should also require more extensive public reporting on the use of FISA, to allow better public oversight, more like the useful reports issued for other criminal wiretap orders.

-- Definition of "domestic terrorism"

The PATRIOT Act's definition of domestic terrorism is a looming problem. Section 802 of the Act defines domestic terrorism as acts dangerous to human life that violate any state or federal criminal law and appear to be intended to intimidate civilians or influence government policy. 18 USC 2331(5). Under the PATRIOT Act, this definition has three consequences - the definition is used as the basis for:

o Seizure of assets (Sec. 806)
o Disclosure of educational records (Secs. 507 and 508)
o Nationwide search warrants (Sec. 219)

The definition appears many more times in Patriot II, where it essentially becomes an excuse for analysis and consideration. Congress should either amend the definition or refrain from using it. It essentially amounts as a transfer of discretion to the Executive Branch, which can pick and choose what it will treat as terrorism, not only in charging decisions but also in the selection of investigative techniques and in the questioning of individuals.

Other Issues Outside the PATRIOT Act

-- Data Mining

In September 2002, a U.S. Army contractor acquired from the JetBlue airline the itinerary information of over 1.5 million passengers, including passenger names, addresses, and phone numbers. The disclosure occurred in apparent violation of JetBlue's privacy promise to its customers and without the necessary Privacy Act notice by the Army, indicating that it was creating a databases of air passenger records. The contractor purchased from a commercial vendor demographic data on many of the JetBlue passengers including gender, home specifics (owner/renter, etc.), years at residence, economic status (income, etc.), number of children, Social Security number, number of adults, occupation, and vehicle information. The contractor then prepared a Homeland Security Airline Passenger Risk Assessment, attempting "to measure the viability of verifying and scoring passengers by checking them against data-aggregation companies' files."

The JetBlue case not only represents an unauthorized invasion of privacy, but also represents the tip of an iceberg on the government's development and use, without adequate guidelines of the technique known as "data mining," which purports to be able to find evidence of possible terrorist preparations by scanning billions of everyday transactions, potentially including a vast array of information about Americans' personal lives such as medical information, travel records and credit card and financial data. The FBI's Trilogy project includes plans for data mining. According to an undated FBI presentation obtained by the Electronic Privacy Information Center, the FBI's use of "public source" information (including proprietary commercial databases) has grown 9,600% since 1992.

Current laws place few constraints on the government's ability to access information for terrorism-related data mining. Under existing law, the government can ask for, purchase or demand access to most private sector data. Unaddressed are a host of questions: Who
should approve the patterns that are the basis for scans of private databases and under what

standard? What should be the legal rules limiting disclosure to the government of the identity of those whose data fits a pattern? When the government draws conclusions based on pattern analysis, how should those conclusions be interpreted? How should they be disseminated and when can they be acted upon?

Adapting the Privacy Act to government uses of commercial databases is one way to look at setting guidelines for data mining. But some of the Privacy Act's principles are simply inapplicable and others need to have greater emphasis. For example, perhaps one of the most important elements of guidelines for data mining would be rules on the interpretation and dissemination of hits and on how information generated by computerized scans can be used. Can it be used to conduct a more intensive search of someone seeking to board an airplane, to keep a person off an airplane, to deny a person access to a government building, to deny a person a job? What due process rights should be afforded when adverse actions are taken against individuals based on some pattern identified by a computer program? Can ongoing audits and evaluation mechanisms assess the effectiveness of particular applications of the technology and prevent abuse?

All of these questions must be answered before moving forward with implementation. As it stands now, Congress doesn't even know how many other JetBlue cases exist, for there is no disclosure of what commercial databases agencies are acquiring. Congress should limit the implementation of data mining until it knows what is going on, the effectiveness of the technique has been shown and guidelines on collection, use, disclosure and retention have been adopted following appropriate consultation and comment.

-- The FBI Guidelines

The FBI is subject to two sets of guidelines, a largely classified set for foreign intelligence and international terrorism investigations ("National Security Investigation (NSI) Guidelines"), and an unclassified set on general crimes, racketeering and domestic terrorism ("Criminal Guidelines"). Last year, the Attorney General changed the Criminal Guidelines. Just last month, he changed the NSI Guidelines, which relate to intelligence investigations of Osama bin Laden and Al Qaeda.

As they now stand amended, neither set of guidelines offers much guidance to FBI agents and supervisors seeking to prioritize and focus their intelligence gathering activities. In the past, the FBI was able to open investigations where there was some specific basis for doing so. Under the Criminal Guidelines, the FBI

was able initiate a full domestic counter-terrorism investigation when facts and circumstances reasonably indicated that two or more people were engaged in an enterprise for the purpose of furthering political goals through violence. Under the old national security guidelines, the FBI was authorized to open an investigation of any international terrorist organization (there was a long-running investigation prior to 9/11 of Osama bin laden's group) and to investigate separately any individual suspected of being a member or supporter of a foreign terrorist organization. FBI agents could conduct quite intrusive preliminary investigations on an even lower standard.

Both sets of guidelines gave agents wide berth. The old guidelines allowed FBI agents to go into any mosque or religious or political meeting if there was reason to believe that criminal conduct was being discussed or planned there or that an international terrorist organization was recruiting there, and, in fact, over the years the FBI conducted terrorism investigations against a number of religious organizations and figures. Separate guidelines even allowed undercover operations of religious and political groups, subject to close supervision.

Now, the FBI is cut loose from that predication standard, with no indication as to how it should prioritize its efforts or avoid chilling First Amendment rights. As the Attorney General has stated, FBI agents can now surf the Internet like any teenager. They can now enter mosques and political meeting on the same basis as any member of the public - on a whim, out of curiosity. Fortunately, FBI agents may have more sense than that. The head of the counter-terrorism efforts was quoted as saying that Al Qaeda was not recruiting in mosques. But the results may be previewed in New York, where there were disturbing reports that local police, shortly after their guidelines were changed, engaged in questioning demonstrators about their political beliefs.

In responding to the issues raised by the guideline changes, Congress should require the adoption, following consultation and comment, of Guidelines for collection, use, disclosure and retention of public event information. Such guidelines should include a provision specifying that no information regarding the First Amendment activities of a US person or group composed substantially of US persons can be disseminated outside the FBI except as part of a report indicating that such person or group is planning or engaged in criminal activity.

Conclusion

In the debate over the PATRIOT Act, civil libertarians did not argue that the government should be denied the tools it needs to monitor terrorists' communications or otherwise carry out effective investigations. Instead, privacy advocates urged that those powers be focused and subject to clear standards and judicial review. The tragedy of the response to September 11 is not that the government has been given new powers - it is that those new powers have been granted without standards or checks and balances.

We need limits on government surveillance and guidelines for the use of information not merely to protect individual rights but to focus government activity on those planning violence. The criminal standard and the principle of particularized suspicion keep the government from being diverted into investigations guided by politics, religion or ethnicity. Meaningful judicial controls do not tie the government's hands - they ensure that the guilty are identified and that the innocent are promptly exonerated.

For more information, contact:
Jim Dempsey
(202) 637-9800 x112
jdempsey@cdt.org
http://www.cdt.org