Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology[1]

before the
Senate Select Committee on Intelligence

April 19, 2005

Mr. Chairman, Sen. Rockefeller, Members of the Committee, thank you for the opportunity to testify at this important hearing. In CDT's view, there are few if any provisions in the PATRIOT Act that are per se unreasonable. We see not a single power in the Act that should sunset. The question before us – and it is one of the most important questions in a democratic society – is what checks and balances should apply to those powers. In our view, the investigative powers of the PATRIOT Act would be just as effective, maybe even more so, if subject to some basic checks and balances –

- particularized suspicion,
- a minimal factual showing,
- judicial approval,
- eventual notice to targets in a wider range of circumstances, and
- more detailed unclassified reporting to Congress.

In particular, we urge the Committee to enhance the role of the judiciary. We fully recognize that intelligence investigations must sometimes proceed with speed and that they often require secrecy. But in this age of cell phones, ubiquitous Internet access, encryption, BlackBerries and other communications technologies, it seems unnecessary to vest domestic intelligence agencies with extra-judicial powers. FBI agents and others operating domestically in intelligence matters – who have to seek supervisory approval for exercise of PATRIOT Act powers in almost all cases anyhow - could electronically prepare minimal fact-based applications for access to information, submit them to judges electronically, and receive approval electronically, promptly, efficiently, but with the crucial check provided by a neutral and detached magistrate.

CDT supports the Security and Freedom Enhancement (SAFE) Act, a narrowly-tailored bipartisan bill that would revise several provisions of the PATRIOT Act. It would retain all of the expanded authorities created by the Act but place important limits on them. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

---

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

Prevention of Terrorism Does Not Require Suspension of Standards and Oversight

At the outset, let me stress some basic points on which I hope there is widespread agreement:

- Terrorism poses a grave and imminent threat to our nation. There are people -- almost certainly some in the United States -- today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.
- The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to conduct electronic surveillance, carry out physical searches effectively, and obtain transactional records or business records pertaining to suspected terrorists.
- These authorities, however, must be guided by the Fourth Amendment, and subject to Executive and judicial controls as well as legislative oversight and a measure of public transparency.

Since 9/11, There Have Been Egregious and Counterproductive Abuses of Civil Liberties and Human Rights Outside the PATRIOT Act

Since 9/11, the federal government has engaged in serious abuses of constitutional and human rights, some now documented in official reports. The most egregious of these abuses have taken place outside of the PATRIOT Act or any other Congressional authorization. These include:

- The torture at Abu Ghraib and other locations.
- The detention of US citizens in military jails without criminal charges.
- The detention of foreign nationals in Guantanamo and other locations, under what the Executive Branch claimed was unreviewable authority, and the continuing detention of those individuals after the Supreme Court rejected the Administration's claims.
- The rendition of detainees to other governments known to engage in torture.
- Haphazard and prolonged post 9/11 detentions of foreign nationals in the U.S., the physical abuse of some and the blanket closing of deportation hearings.
- Abuse of the material witness law to hold individuals in jail without charges.

Concerns with the PATRIOT Act: Intelligence Searches -- Broader Scope and Greater Secrecy Call for Compensating Controls

In the PATRIOT Act, not surprisingly given the pressures under which that law was enacted and the lack of considered deliberation, the pendulum swung too far, and Congress eliminated important checks and balances that should now be restored in the interest of both freedom and security. One of the most fundamental themes of the PATRIOT Act was the elimination of checks and balances on intelligence access to financial, communications and other records.

As this Committee well knows, the FBI operates under two sets of authorities when investigating international terrorism: criminal and foreign intelligence/counterintelligence. Over the past 25 years, a series of intelligence authorities have grown up giving investigators the ability to conduct electronic surveillance and obtain access to stored records.

Constitutionally speaking, there are two concerns with national security authorities:

- The scope of intelligence investigations is broader than criminal investigations. Intelligence investigations cover both legal and illegal activities. In criminal investigations, the criminal code provides an outer boundary, and a prosecutor is often involved to guide and control the investigation. An intelligence investigation is driven not by a desire to arrest and convict, but by a range of foreign policy interests. The breadth of disclosure of information is greater, including intelligence, military, diplomacy, policy development, protective, immigration, and law enforcement.

- Intelligence investigations require a greater degree of secrecy than criminal investigations. In criminal cases, an important protection is afforded by notice to the target and other affected parties as the government collects information and the notice and right to confront when a matter reaches trial. Under the intelligence rules, persons whose records are accessed by the government are never provided notice unless the evidence is introduced against them in court. While recipients of grand jury subpoenas can publicly complain about overbreadth and often can even notify the target, recipients of intelligence disclosure orders are barred from disclosing their existence.

The PATRIOT Act failed to include protections that can respond to these difference and provide appropriate protection of Fourth Amendment principles.

-- **Particularized suspicion and a factual basis for disclosure demands**

In the PATRIOT Act, Sections 214 (relating to pen registers under FISA), 215 (relating to travel records and other business records) and 505 (relating to National Security Letters for credit reports, financial records and communications transactional data) all pose the same set of issues. Prior to the PATRIOT Act, the FBI was able to obtain access to certain key categories of information upon a showing that the information pertained to a foreign power or an agent of a foreign power:

- Real time interception of transactional data concerning electronic communications was available with a pen register or trap and trace order issued by the FISA court.
- Records regarding airline travel, vehicle rental, hotels and motels and storage facilities were available with a court order issued by the FISA court.
- Financial records, credit reports, and stored transactional records regarding telephone or Internet communications were available with a National Security Letter issued by a senior FBI official.

In all cases, prior to PATRIOT, these records were available upon a certification or showing that there were "specific and articulable facts" giving reason to believe that the person whose records were being sought was a foreign power or an agent of a foreign power, or had been in contact with a foreign power or its agent. The FBI complained that this standard was too narrow. Rather than come up with a focused standard, the PATRIOT Act eliminated both prongs of this standard: It eliminated the particularity requirement; and it eliminated the requirement that the FBI have any factual basis for its interest in certain records.

FBI and DOJ descriptions of these changes in guidance to the field and in statements to Congress suggest that the government does not interpret them as going as far as they seem to on their face. The FBI indicates that it still names particular subjects in its applications, and both DOJ and FBI indicate that there is some factual basis for every request.

The fact that records must be relevant to an open investigation is not any real protection at all. Consider the following: there is undoubtedly a properly authorized FCI investigation of al Qaeda (or UBL). Under sections 214, 215 and 505, the FBI could get any records from any entity by claiming that they were relevant to that investigation. Even though 215 requires a court order, the statute requires the judge to grant the governments request in whole or part so long as the government makes the proper assertion - that the records are sought for an existing investigation, however broad that investigation. There is no requirement that the application or the court order or NSL name the person or account for which information is sought.

Both the particularity requirement and the factual showing requirement should be made explicit in statute, in order to prevent overbroad or ill-focused searches and to provide clear guidance to the field and the FISA court.

At the same time, the concept of a National Security Letter should be revisited. in this age of cell phones, ubiquitous Internet access, encryption, BlackBerries and other communications technologies, it seems unnecessary to vest domestic intelligence agencies with extra-judicial powers. FBI agents and others operating domestically in intelligence matters – who have to seek supervisory approval for exercise of PATRIOT Act powers in almost all cases anyhow - could electronically prepare minimal fact-based applications for access to information, submit them to judges electronically, and receive approval electronically, promptly, efficiently, but with the crucial check provided by a neutral and detached magistrate.

-- **Notice**

A second area in which the PATRIOT Act lacks adequate protections is in the area of notice. Under the PATRIOT Act, as in the past, intelligence authorities are exercised under a cloak of perpetual secrecy. In the world of spy versus spy, surveillances could go on for many years, the same techniques could be used in the same context for decades, and known spies would be allowed to operate with no overt action ever taken against them. To a certain

extent, these secrecy interests remain paramount in counter-terrorism investigations. But the wall between intelligence and criminal has now been brought down, and information collected in intelligence investigations is now being ever more widely shared and used. The question of when and how individuals are provided notice needs to be reexamined. Especially individuals whose records were obtained by the government but who were later determined not to be of any interest to the government should be told of what happened to them.

In ordinary criminal investigations, the PATRIOT Act created what might be called "off the books surveillance." Section 212 authorizes an ISP to disclose email, stored voicemail, draft documents and other stored information to law enforcement when government states that there is an emergency involving a threat to life. Section 217 authorizes the government to carry out real-time surveillance when an ISP, a university, or another system operator authorizes the surveillance on the grounds that there is a "trespasser" within the operator's computer network. Under both sections 212 and 217,

- There is never a report to a judge. (In contrast, under both Title III and FISA, when electronic surveillance is carried out on an emergency basis, an application must be filed after the fact.)
- There is no time limit placed on the disclosures or interceptions. (A Title III wiretap cannot continue for more than 30 days without new approval.)
- There is never notice to the person whose communications are intercepted or disclosed.
- The interceptions and disclosures are not reported to Congress.

DOJ, in its defense of Section 217 claims that the privacy of law-abiding computer users is protected because only the communications of the computer trespasser can be intercepted. But what if the system operator is wrong? What if there is a legitimate emergency, but law enforcement targets the wrong person. Under Sections 212 and 217, a guilty person gets more notice than an innocent person – the guilty person is told of the surveillance or disclosure but the innocent person need never be notified. That should be rectified.

-- Congressional Oversight and Public Reporting

Currently, the Justice Department is required to report to Congress on its use of some sections of the PATRIOT Act, such as its use of Section 215, but it is not required statutorily to report on its use of other sections. Although the Justice Department, under the pressure of the sunsets and with considerable prodding from Congress, has voluntarily reported some information on its use of other PATRIOT Act powers, like delayed notice warrants under Section 213, routine and more detailed reporting would increase both Congressional oversight and public transparency. Congress should codify reporting requirements, enabling Congress and the public to assess the efficacy of these provisions and to gauge the likelihood of their misuse.

Specific Provisions of the PATRIOT Act

In this section, we will comment on specific provisions of the PATRIOT Act.

-- **Sneak and Peek Searches**

Section 213, which does not sunset but nevertheless should be reexamined, is a good idea gone too far. It is also a perfect example of how the PATRIOT Act was used to expand government powers, without suitable checks and balances, in areas having nothing to do with terrorism. Finally, it illustrates how, when rhetoric is left behind, it is possible to frame appropriate checks and balances for what, by any definition, are some especially intrusive powers.

As a starting point, of course, in serious investigations of international terrorists, the government should be able to act with secrecy. But guess what proponents of Section 213 never mention? In international terrorism investigations, even before the PATRIOT Act, the government already had the authority to carry out secret searches. The Foreign Intelligence Surveillance Act was amended in 1994 to allow secret searches in intelligence investigations, including international terrorism cases; before 1994, the Attorney General authorized secret searches in intelligence investigations of terrorist groups without any judicial scrutiny. And during the limited debate over the PATRIOT Act, reasonable voices proposed that secret searches be statutorily authorized in criminal investigations of terrorism.

As enacted, however, Section 213 was not limited to terrorism cases. 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. It would especially astound them that this authority is available for all federal offenses, ranging from weapons of mass destruction investigations to student loan cases. That is what Section 213 of the PATRIOT Act authorizes. Indeed, the Justice Department has admitted that it has used 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 standards, courts had allowed delayed notice or sneak and peek searches. The term "sneak and peek," by the way, was not contrived by opponents of the PATRIOT Act – before the PATRIOT Act, it was used by FBI agents, DOJ officials, and judicial opinions. Rather than "codifying existing case law under a single national standard to streamline detective work," Section 213 confuses the law. Rather than trying to devise a standard suitable to breaking and entering into homes and offices for delayed notice searches, Congress

in the haste of 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 lower 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 rules. "Reasonable period" affords judges considering sneak and peek sneak and peek searches no uniform standard.

If, as Section 213 supporters claim, sneak and peek searches are a "time-honored tool," and if courts "around the country have been issuing them for decades," as DOJ claims, why did the Justice Department push so hard in the PATRIOT Act for a Section 213 applicable to all cases? The answer, I believe, is that the sneak and peek concept stands on shaky constitutional ground, and the Justice Department was trying to bolster it with Congressional action – even action by a Congress that thought it was voting on an anti-terrorism bill, not a general crimes bill.

The fact is, there is a constitutional problem with Section 213: The sneak and peek cases rest on an interpretation of the Fourth Amendment that is no longer valid. 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.). These 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 ... ."

Yet in *Wilson v. Arkansas*, 514 U.S. 927 (1995), in a unanimous opinion by Justice Thomas, the Supreme Court held that the knock and notice requirement of common law was incorporated in the Fourth Amendment as part of the constitutional inquiry into reasonableness. Notice is part of the Fourth Amendment, the court held, directly repudiating the premise 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 at all. 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.

Section 213's attempted codification of the sneak and peek authority went too far. To fix it, Congress should leave the statutory authority in place but add several limitations:

- Congress should narrow the circumstances in which notification may be delayed so that Section 213 does not apply to virtually every search. Under Section 213, the government need only show that providing notice would seriously jeopardize an investigation or unduly delay a trial. This "catch-all" standard could apply in almost every case and therefore is simply too broad for this uniquely intrusive type of search. Congress should allow sneak and peek searches only if giving notice would likely result in: danger to the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; or intimidation of potential witnesses.

- Congress should require that any delay in notification not extend for more than seven days without additional judicial authorization. Section 213 permits delay for a "reasonable time" period, which is undefined in the statute. Pre-PATRIOT Act case law in the Ninth and Second Circuits stated that seven days was an appropriate time period. Indeed, DOJ's internal guidance recognizes that seven days is the most common period, but also suggests that it may seek much longer delays. Congress should set a basic seven day rule, while permitting the Justice Department to obtain additional seven-day extensions of the delay if it can continue to meet one of the requirements for authorizing delay in the first instance.

- Section 213 only requires a judge to find "reasonable cause" to believe that an adverse result will happen if notice is not delayed. The Supreme Court has allowed a limited exception to the notice rule upon "reasonable suspicion," by allowing police to enter and provide notice *as they were entering* when they faced a life-threatening situation in executing a warrant. Richards v. Wisconsin, 520 U.S. 385 (1997). If "reasonable suspicion" is the standard for delaying notice by minutes, probable cause would be a more appropriate standard when notice is delayed for days or weeks.

- Finally, Congress should require the Justice Department to continue to report on its use of the "sneak and peek" power. Congress should codify a requirement that the Attorney General report the number of requests for delayed notification, the number of those requests granted or denied, the number of extensions requested, granted and denied, and the prong of the statutory test used for each case, so that Congress and the public can determine if this technique is being narrowly applied.

Even with these changes, sneak and peek searches, especially of homes, stand on shaky constitutional ground except in investigations of the most serious crimes. Judicial caution is necessary. The reasonable changes outlined above would leave the statutory authority in place but bring it under more appropriate limitations and oversight

-- **Section 215 - Business Records**

As noted above, 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, but 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, 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.

-- **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. 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. 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:

- Seizure of assets (Sec. 806)
- Disclosure of educational records (Secs. 507 and 508)
- 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.

SAFE ACT

CDT strongly supports the Security and Freedom Enhancement (SAFE) Act is a narrowly-tailored bipartisan bill that would revise several provisions of the USA PATRIOT Act. It would retain all of the expanded authorities created by the PATRIOT Act but place important limits on these authorities. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

-- **Section 2 – FISA Roving Wiretaps (Section 206 of the PATRIOT Act)**

The SAFE Act would retain the PATRIOT Act's authorization of roving wiretaps and "John Doe" wiretaps under the Foreign Intelligence Surveillance Act (FISA), but would eliminate "John Doe" roving wiretaps, a sweeping power never before authorized by Congress. A "John Doe" roving wiretap does not identify the person or the phone to be wiretapped. The SAFE Act would also require law enforcement to ascertain the presence of the target of the wiretap before beginning surveillance. This would protect innocent Americans from unnecessary surveillance.

-- **Section 3 – "Sneak & Peek" Searches (Section 213)**

The SAFE Act would retain the PATRIOT Act's authorization of delayed notification or "sneak and peek" searches when one of an enumerated list of specific, compelling reasons to delay notice is satisfied. However, it would eliminate the catch-all provision that allows sneak and peek searches in any circumstances seriously jeopardizing an investigation or unduly delaying a trial. The SAFE Act would require notification of a covert search within seven days, instead of the undefined delay that is currently permitted by the PATRIOT Act. A court could allow unlimited additional 21-day delays of notice in specific, compelling circumstances.

Section 4 – FISA Orders for Library and Other Personal Records (Section 215)

The SAFE Act would retain the PATRIOT Act's expansion of the FISA records provision, which allowed the FBI to obtain "any tangible things" from any entity. However, it would restore a standard of individualized suspicion for obtaining a FISA order and create procedural protections to prevent abuses. The government would be able to obtain an order if they could show facts indicating a reason to believe the tangible things sought relate to a suspected terrorist or spy. As is required for grand jury subpoenas, the SAFE Act would give the recipient of a FISA order the right to challenge the order, require a showing by the government that a gag order is necessary, place a time limit on the gag order (which could be extended by the court), and give a recipient the right to challenge the gag order. The SAFE Act would require notice to the target of a FISA order if the government seeks to use the things obtained from the order in a subsequent proceeding, and give the target an opportunity to challenge the use of those things. Such notice and challenge provisions are required for other FISA authorities (wiretaps, physical searches, pen registers, and trap and trace devices).

-- **Section 5 – National Security Letters (Section 505)**

The SAFE Act would restore a standard of individualized suspicion for using an NSL, requiring that the government have reason to believe the records sought relate to a suspected terrorist or spy. As is the case for grand jury subpoenas, the SAFE Act would give the recipient of an NSL the right to challenge the letter and the nondisclosure requirement, and place a time limit on the nondisclosure requirement (which could be extended by the court). As is the case for FISA authorities, the SAFE Act would give notice to the target of an NSL if the government seeks to use the records obtained from the NSL in a subsequent proceeding, and give the target an opportunity to challenge the use of those records.

-- **Section 6 – Pen Registers and Trap and Trace Devices (Section 216)**

The SAFE Act would retain the PATRIOT Act's expansion of the pen/trap authority to electronic communications. In recognition of the vast amount of sensitive information that law enforcement can now access, the SAFE Act would create modest safeguards allowing increased Congressional, public, and judicial oversight of pen/trap usage. The SAFE Act would require additional Congressional reporting, require delayed notice to individuals who are targets of pen/traps (pen/trap targets currently receive no notice, unlike the targets of wiretaps), and slightly raise the burden of proof for obtaining pen/trap orders. Under the current standard, the government need only certify that the information sought is relevant, a certification that a judge has no power to question. Under the revised standard, the government would have show to facts indicating a reason to believe that the information sought is relevant.

-- **Section 7 – Domestic Terrorism Definition (Section 802)**

The PATRIOT Act's overbroad definition of domestic terrorism could include acts of civil disobedience by political organizations. While civil disobedience is and should be illegal, it is not necessarily terrorism. The SAFE Act would limit the qualifying offenses for domestic terrorism to those that constitute a federal crime of terrorism, instead of any federal or state crime, as is currently the case.

-- **Section 8 – FISA Public Reporting**

The PATRIOT Act made it much easier for law enforcement to use FISA to conduct secret surveillance on American citizens regardless of whether they are suspected of involvement in terrorism or espionage and whether the primary purpose of the underlying investigation is intelligence gathering. In 2003, the most recent year for which statistics are available, the number of FISA wiretaps exceeded the number of criminal wiretaps for the first time since FISA became law. It is important for Congress and the American people to learn more about how the FBI is using FISA since the passage of the PATRIOT Act. Therefore, the SAFE Act would require increased public reporting on the use of FISA.

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.

- 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, under both the criminal wiretap law and under FISA, 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 FISA evidence in criminal cases should not be shielded from the adversarial process (as it has been in every case to date).

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
http://www.cdt.org

APPENDIX – Overview of PATRIOT Sunsets

Of over 150 provisions in the PATRIOT Act, only 16 provisions are covered by the sunset. Some of those covered are uncontroversial, while some of the most controversial provisions in the Act are not slated to sunset. The sunset does not apply to pending investigations.

Here's what the sunset covers – **bold** indicates those that are controversial in CDT's view – we have no objections to the others:

Sec. 201 – certain terrorism crimes as wiretap predicates
Sec. 202 – computer fraud as wiretap predicate
Sec. 203(b) – sharing criminal wiretap information w/ intelligence agencies
Sec. 204 – technical clarification of no conflict between Title III and FISA
Sec. 206 – roving taps under FISA
Sec. 207 – extending duration of FISA taps of non-us persons
Sec. 209 – seizure of voice mail pursuant to warrant
Sec. 212 – emergency disclosures of email w/o a court order
Sec. 214 – lowering standard for pen registers and trap and trace devices under FISA
Sec. 215 – access to business records under FISA (the "library records" provision)
Sec. 217 – interception of computer trespasser communications w/o a court order
Sec. 218 – the "significant purpose" provision
Sec. 220 – nationwide service of search warrant for electronic evidence
Sec. 223 – civil liability for unauthorized disclosures of wiretap info
Sec. 224 – the sunset provision itself
Sec. 225 – immunity for compliance with FISA wiretap

A number of highly controversial PATRIOT provisions are not covered by the sunset, and deserve to be reconsidered by Congress, including:

Sec 203(a) – sharing grand jury information
Sec. 213 – sneak and peek searches
Sec. 216 – pen registers for the Internet
Sec. 358 – exceptions to the financial privacy laws
Sec. 505 – "National Security Letter" exceptions to privacy laws
Sec. 802 – definition of domestic terrorism