WASHINGTON
LEGISLATIVE OFFICE


American Civil Liberties Union

**AMERICAN CIVIL LIBERTIES UNION**
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
*DIRECTOR*

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500



Testimony at a Hearing on the

# USA PATRIOT Act of 2001

Before the

Permanent Select Committee on Intelligence

of the

House of Representatives

Submitted by

Timothy H. Edgar
National Security Policy Counsel

May 11, 2005

**American Civil Liberties Union**
**Testimony at a Hearing on the USA PATRIOT Act of 2001**
**before the House Permanent Select Committee on Intelligence**
**Submitted by Timothy H. Edgar, National Security Policy Counsel**

**May 11, 2005**

Chairman Hoekstra, Ranking Member Harman and Members of the Committee:

I am pleased to appear before you today on behalf of the American Civil Liberties Union and its more than 400,000 members, dedicated to preserving the principles of the Constitution and Bill of Rights at this rare, and crucial, public oversight hearing on the USA PATRIOT Act of 2001.[1]

The Patriot Act was passed by Congress in 2001 just six weeks after the terrorist attacks of September 11. Although the act passed by wide margins, members on both sides of the aisle expressed reservations about its impact on fundamental freedoms and civil liberties. As a result, Congress included a "sunset clause" providing that over a dozen provisions will expire on December 31, 2005, if Congress does not act to renew them.

Congress was wise to do so. Terrorism has been with us for a long time. It will likely be with us for generations to come. The decisions that you make over the coming months about the Patriot Act must be made with an eye toward that reality.

A number of the provisions that will expire are within the jurisdiction of this committee, including some of the most controversial provisions. This statement's main focus is on those Patriot Act intelligence provisions that pose the greatest risk for civil liberties.[2]

Congress should use the upcoming debate over the renewal of parts of the Patriot Act as an opportunity to reassert its rightful role in determining law enforcement and national security policy in the post-9/11 context, which has waned as the power of the Executive Branch has waxed. Before re-authorizing any intelligence power, this committee should require the Executive Branch to meet the standard articulated by the bipartisan 9-11 Commission.

- First, Congress should re-examine the specific provisions that sunset, taking care not to renew any provision unless the government can show "(a) that the power actually materially enhances security and (b) that

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.
[2] This statement is adapted from a longer memorandum that examines a number of other Patriot Act and related issues in greater depth, including immigration, material witness and "enemy combatant" detentions, criminal "sneak and peek" search warrants, the crime of material support of terrorism and the definition of domestic terrorism. *See* Memo to Interested Persons Outlining What Congress Should Do About the Patriot Act Sunsets, March 28, 2005, available at: http://www.aclu.org/news/NewsPrint.cfm?ID=17846&c=206

there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties."[3]

- Second, "[i]f the power is granted, there must be adequate guidelines and oversight to properly confine its use."[4]

Congress may not be able to fully review or assess the effectiveness, and impact on civil liberties, of some anti-terrorism powers that the Executive Branch was granted in the Patriot Act. The lack of meaningful information about the use of many powers is sometimes a direct result of excessive secrecy in the Executive Branch, and sometimes the result of necessary secrecy. In any case where sufficient information is not available to undertake a thorough review, Congress should set a new sunset date and impose additional reporting requirements to facilitate a proper review, rather than cede those powers permanently to the Executive Branch.

Because many domestic intelligence authorities operate in complete secrecy, this committee plays a particularly critical role in determining whether specific intelligence powers "actually materially enhance security." Only an intensive and painstaking process of examining the facts regarding the use of these powers can answer that question.

This committee was created in large part to perform just that function. It should not be content with general statements of the Patriot Act's usefulness or selective accounts of how certain sections have been used. Rather, we hope it will aggressively and thoroughly examine whether administration claims that certain powers are vital to the prevention of terrorism are born out by specific facts.

Until now, the government has fallen short. Last month, Senate Judiciary Chairman Arlen Specter expressed frustration at the Justice Department's inability to provide such facts even in a classified setting. "This closed-door briefing was for specifics," Senator Specter explained. "They didn't have specifics." [5]

*Excessive Secrecy Impedes Oversight of Patriot Act*

Secrecy permeates the Patriot Act, particularly in its expansions of intelligence authorities. Many powers are accompanied by statutory gag orders. Moreover, the administration has taken the posture that information that is embarrassing to it must be kept secret for reasons of national security. For these reasons, it has been extremely difficult to uncover information about how the Patriot Act has been used, and even information about whether particular sections have been

[3] Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission Report") 294-95 (2004) (boldfaced recommendation)
[4] *Id.*
[5] Eric Lichtblau, *Specter Voices Frustration Over Briefing on Patriot Act*, N.Y. Times, Apr. 13, 2005.

used at all. The ACLU has repeatedly sought this information in letters, requests under the Freedom of Information Act (FOIA) and in FOIA litigation.

Despite the efforts of the Executive Branch to conceal information about how controversial provisions of the Patriot Act have been used, some information has become public. This information is disturbing in and of itself, and may be emblematic of other abuses that have not yet become public. Appended to this testimony are some examples of abuses of intelligence powers expanded under the Patriot Act, and of the chill on the exercise of First Amendment rights that such powers can create.

*Patriot Act Intelligence Powers: Greater Secrecy, Less Meaningful Review*

In the debate over the Patriot Act, we ask the committee to pay particular attention to the most intrusive expanded intelligence surveillance techniques.

Secret Records Searches Without Probable Cause or an Ability to Challenge: Library Records, Other "Tangible Things," and National Security Letters

Perhaps no sections of the Patriot Act have become more controversial than the sections allowing the government secretly to obtain confidential records in national security investigations – investigations "to protect against international terrorism or clandestine intelligence activities."

National security investigations are not limited to gathering information about criminal activity. Instead, they are intelligence investigations designed to collect information the government decides is needed to prevent – "to protect against" – the threat of terrorism or espionage. They pose greater risks for civil liberties because they potentially involve the secret gathering of information about lawful political or religious activities that federal agents believe may be relevant to the actions of a foreign government or foreign political organization (including a terrorist group).

The traditional limit on national security investigations is the focus on investigating foreign powers or agents of foreign powers. Indeed, the "foreign power" standard is really the only meaningful substantive limit for non-criminal investigations given the astonishing breadth of information government officials might decide is needed for intelligence reasons. The Patriot Act eliminated this basic limit for records searches, including the power under the Foreign Intelligence Surveillance Act (FISA) to obtain with a FISA court order any records or other "tangible things," and the FBI's power to obtain some records without any court review at all.

- Section 215 of the Patriot Act allows the government to obtain any records, e.g., library and bookseller records, medical records, genetic information, membership lists of organizations, and confidential records of refugee service organizations, as well as any other "tangible things" with an order from the FISC. The order is based merely on a certification by the government that the records are "sought for" a

national security investigation and the judge is required to issue the order. The order contains an automatic and permanent gag order. Section 215 is subject to the sunset clause. Last month, the government acknowledged for the first time that Section 215 has been used, that it has been used 35 times, and that it was used to obtain credit, apartment, ISP and other records, but not library or medical records.

- Section 505 of the Patriot Act expanded the FBI's power to obtain some records in national security investigations without any court review at all. These "national security letters" can be used to obtain financial records, credit reports, and telephone, Internet and other communications billing or transactional records. The letters can be issued simply on the FBI's own assertion that they are needed for an investigation, and also contain an automatic and permanent nondisclosure requirement. Section 505 does not sunset.

Although such demands never required probable cause, they did require, prior to the Patriot Act, "specific and articulable facts giving reason to believe" the records pertain to an "agent of a foreign power." The Patriot Act removed that standard for issuing records demands in national security investigations.

As a result, a previously obscure and rarely used power can now be used far more widely to obtain many more records of American citizens and lawful residents. Because the requirement of individual suspicion has been repealed, records powers can now be used to obtain entire databases of private information for "data mining" purposes – using computer software to tag law abiding Americans as terrorist suspects based on a computer algorithm.

These records search provisions are the subject of two court challenges by the ACLU. In *Muslim Community Association of Ann Arbor* v. *Ashcroft*, No. 03-72913 (E.D. Mich.), the ACLU has challenged section 215 of the Patriot Act on First and Fourth Amendment grounds. As explained in the case example, the ACLU's challenge has uncovered serious and unconstitutional chilling effects of section 215 on the exercise of basic freedoms. The district court has not yet ruled in this case.

In *Doe* v. *Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a federal district court struck down a "national security letter" records power expanded by the Patriot Act, agreeing with the ACLU that the failure to provide any explicit right for a recipient to challenge a national security letter search order violated the Fourth Amendment and that the automatic secrecy rule violated the First Amendment. The case is now on appeal before the United States Court of Appeals for the Second Circuit.

There has been some confusion about whether *Doe v. Ashcroft* struck down a provision of the Patriot Act. In fact, *Doe v. Ashcroft* struck down, in its entirety, 18 U.S.C. § 2709(b), the national security letter authority for customer records of communications service providers, as amended by section 505(a) of the Patriot Act. The court referred repeatedly to the Patriot Act in its opinion. To be

clear, the court invalidated *all of section 505(a) of the Patriot Act.* It is simply inaccurate to imply that the court's decision was unrelated to the Patriot Act, or that it did not strike down a provision of the Patriot Act. If the court's decision is sustained on appeal, section 505(a) of the Patriot Act will no longer have any force or effect.[6]

Both FISA records demands and national security letters can be used to obtain sensitive records relating to the exercise of First Amendment rights. A FISA record demand can now be used to obtain a list of the books or magazines someone purchases or borrows from the library. A FISA record demand can also now be used to obtain the membership list of a controversial political or religious organization. A national security letter could be used to monitor use of a computer at a library or Internet café under the government's theory that providing Internet access (even for free) makes an institution a "communications service provider" under the law.

While both national security letters and FISA records demands cannot be issued in an investigation of a United States citizen or lawful permanent resident if the investigation is based "solely" on First Amendment activities, this provides little protection. An investigation is rarely, if ever, based "solely" on any one factor; investigations based in large part, but not solely, on constitutionally protected speech or association are implicitly allowed. An investigation of a temporary resident can be based "solely" on First Amendment activities, and such an investigation of a foreign visitor may involve obtaining records pertaining to a United States citizen. For example, a investigation based solely on the First Amendment activities of an international student could involve a demand for the confidential records of a student political group that includes United States citizens or permanent residents.

The government defends section 215 as analogous to a grand jury subpoena in a criminal investigation, which they point out does not require probable cause and can be issued, unlike a section 215 order, without prior review by a judge. As explained above, section 215 is dramatically different from a subpoena because it provides no explicit right to challenge and contains an automatic, permanent gag order that even the Attorney General concedes should be amended to ensure it permits conversations with attorneys.

Moreover, this argument fundamentally misunderstands the difference between foreign intelligence and criminal investigations, and the impact of that difference on First Amendment freedoms. Foreign intelligence investigations

[6] While the use of national security letters are secret, the press has reported a dramatic increase in the number of letters issued, and in the scope of such requests. For example, over the 2003-04 holiday period, the FBI reportedly obtained the names of over 300,000 travelers to Las Vegas, despite casinos' deep reluctance to share such confidential customer information with the government. It is not clear whether the records were obtained in part with a national security letter, with the threat of such a letter, or whether the information was instead turned over voluntarily or to comply with a subpoena.

are domestic investigations of the activities of foreign governments or organizations, including foreign terrorist organizations. Foreign intelligence investigations may involve investigation of criminal activities, such as espionage or terrorism, but may also involve intelligence gathering for foreign policy or other purposes involving lawful activities. The guidelines for conducting foreign intelligence investigations (including what level of suspicion is required for certain intrusive techniques) are classified.

As Justice Powell, writing for the Supreme Court in a landmark case involving intelligence gathering, observed:

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. . . History abundantly documents the tendency of Government--however benevolent and benign its motives--to view with suspicion those who most fervently dispute its policies. . . .
>
> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power.[7]

Moreover, as a result of section 203 of the Patriot Act, information properly obtained in a criminal investigation of terrorism (including information obtained with a grand jury subpoena) can be freely shared with intelligence agents. Section 215 is an entirely different, and more intrusive, power – a power for intelligence agents to obtain highly personal records unbounded by any need to show relevance to any criminal investigation.

The administration has also tried to allay fears about the broad scope of section 215 by selectively disclosing fragmentary information about its use. At a hearing before the Senate Judiciary Committee, Attorney General Gonzales revealed that section 215 had been used 35 times, and had not been used to obtain library or medical records. Of course, once is too often where the underlying statute is unconstitutional, as is the case with section 215. The administration defends the potential use of section 215 to obtain library or other highly personal records without any individual suspicion.

The selective disclosure of information about how often section 215 has been used, and what records it has been used to obtain, calls into serious question the government's longstanding position that such information is properly kept secret. If such aggregate information can be disclosed as part of an aggressive call for Congress to renew the Patriot Act, it can be disclosed in a more balanced and systematic way.[8]

---

[7] *United States v. United States District Court*, 407 U.S. 297, 313-14 (1972).

[8] Section 8 of S. 737, the "Security and Freedom Enhancement Act," requires that the annual number of section 215 searches be made available in a public report along with information about other FISA powers, including the annual number of physical searches, electronic surveillance orders, "lone wolf" surveillance orders, and pen/trap searches.

We do not ask that you repeal either section 215 or section 505 of the Patriot Act. Rather, we ask that restore the "agent of a foreign power" requirement and that you amend the statute to time limit the gag, exempt attorney-client communications from it, and allow for court challenges. If these changes are made to the NSL statute, they would satisfy the court that struck down that statute under the First and the Fourth Amendment.

The SAFE Act ("Security and Freedom Ensured Act," H.R. 1526) restores the requirement of "specific and articulable facts giving reason to believe" the records "pertain to a foreign power or an agent of a foreign power" for FISA records demands and provides a sunset date for the expanded national security letter power. Restoring this requirement is needed to ensure sections 215 and 505 of the Patriot Act are not used to obtain the personal records of ordinary Americans.

The Senate version of the SAFE Act (S. 737) makes additional improvements which should be added to the House version should the SAFE Act move forward to committee consideration. S. 737 makes explicit the right to file a motion to quash the records demands because they are unreasonable, contrary to law, or seek privileged information. The Senate bill also sets standards for a judicially-imposed, temporary secrecy order that can be challenged by the recipient of a records demand. Finally, the Senate bill provides a right to notice, and an opportunity to challenge, before information from a FISA records search or national security letter search can be used in a court proceeding.

Secret Searches and Surveillance of Homes and Offices

A government search or electronic surveillance of a home or office generally requires a warrant based on probable cause of crime under the Fourth Amendment. As a general rule, the owner of the home or office is entitled to notice of the search. Foreign intelligence searches have been an exception to this rule. They do not require criminal probable cause and forbid notice to the owner.

The special power to secretly search a home or office, without ever notifying the owner, is among the most intrusive domestic surveillance powers available to the federal government. Such "black bag jobs" were the hallmark of national security investigations run amok, including COINTELPRO and other investigations of civil rights activists, anti-war activists, and other Americans who in the end were guilty of nothing more than peacefully opposing government policies.

The inappropriate use of a secret search power, without court oversight, led directly to warrantless wiretaps of civil rights leaders and, eventually, an unauthorized "black bag job" at the Watergate, sending a shock wave through the nation and prompting thorough and searching reviews of the intelligence community. These reviews led Congress to enact important reforms of intelligence powers, including the passage of the Foreign Intelligence Surveillance Act (FISA) and the creation of this committee.

While FISA secret searches and wiretaps pre-date the Patriot Act, two vital protections that cabined such searches until 2001 have been seriously eroded by amendments that are subject to the December 31, 2005 sunset. First, section 218 of the Patriot Act allowed the government to obtain a FISA secret search order even where the "primary purpose" of the search was *not* foreign intelligence. Second, for searches of so-called "lone wolf" terror suspects, section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004[9] eliminated, for the first time, the basic requirement applied by the Foreign Intelligence Surveillance Court for all FISA secret searches and surveillance: that probable causes exists that the target of the search is a foreign power or agent of foreign power.

*Section 218 of the Patriot Act.* This provision of the Patriot Act takes aim at a provision of FISA designed to ensure against the government using FISA improperly as an end-run around the Fourth Amendment for criminal suspects. Prior to the Patriot Act, government officials had to certify that the *primary purpose* of a secret FISA search was to obtain foreign intelligence.[10] Section 218 of the Patriot Act weakened this standard, allowing agents to obtain these warrants so long as they certify that "*a significant purpose*" of the search is foreign intelligence.

The danger of section 218's lower standard is that the government will cut corners in criminal cases. Because foreign intelligence no longer must be the primary purpose of the search, the government can use FISA as a substitute for traditional criminal powers. As a result, now the government can -- for what are primarily criminal searches -- evade the Fourth Amendment's constraints of probable cause of crime and notice to the person whose property is being searched.

Brandon Mayfield is a case where such corners may have been cut. As described in more detail in the appendix, Mr. Mayfield is a Portland, Oregon resident who is a convert to Islam and a civil rights advocate. Mr. Mayfield was wrongly accused by the government of involvement in the Madrid bombing as a result of a evidence, including a mistaken fingerprint identification, that fell apart after the FBI re-examined its case following its arrest and detention of Mr. Mayfield on a material witness warrant.

As Attorney General Gonzales acknowledged at a hearing before the Senate Judiciary Committee, Section 218 of the Patriot Act was implicated in the secret search of Mr. Mayfield's home. The FBI secretly entered the home of an innocent man it wrongly suspected of a crime without a warrant based on criminal probable cause. It did so because the Patriot Act had made it easier to

[9] Pub. L. No. 108-458, 118 Stat. 3638.

[10] The pre-Patriot Act statute required the government to certify that foreign intelligence was "the purpose" of the search. Where the government had both foreign intelligence and criminal investigation purposes, courts interpreted this language to mean that foreign intelligence purpose had to be the "primary purpose" of the search; otherwise, the government should use its criminal powers. *See In Re Sealed Case*, 310 F.3d 717, 726 (For. Intel. Surv. Ct. Rev. 2002) (collecting pre-Patriot Act cases).

conduct such a search with a FISA search order. While there, agents took hundreds of photographs, copied four computer hard drives and seized ten DNA samples. Prior to the Patriot Act, it is doubtful the search could have taken place under FISA, and instead would likely have been governed by normal search warrant procedures and the exacting standard of criminal probable cause.

The Justice Department maintains that the Mayfield search likely would have been approved before the Patriot Act, because it could have argued the "primary purpose" of its secret search was to gather foreign intelligence information, rather than to gather evidence to use against Mr. Mayfield. While it is impossible to know for certain whether the FISC would have agreed, it is certain that the FISC would have required the Justice Department to prove that the main purpose of a search that was so obviously directed at a criminal suspect was actually to collect foreign intelligence information. The Patriot Act allowed the Justice Department to evade that requirement, and the Department has not shown it could have met it. The Inspector General's investigation of the Mayfield matter is still ongoing.

The Mayfield case and the danger of similar future abuses shows the need for additional safeguards. Without re-building the much-maligned "wall" between foreign intelligence and criminal investigations, Congress should follow the approach of the Foreign Intelligence Surveillance Court (FISC), restoring its power to serve its proper supervisory function to prevent the misuse of FISA. Congress should empower the court to make sure foreign intelligence investigations are not directed by federal prosecutors, although prosecutors and criminal investigators should be allowed full briefings on such investigations.

In its first (and, so far, only) public opinion, the FISC, in an opinion by Judge Lamberth, expressed alarm at the fact that "criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause)" of crime, and noting its highly intrusive aspects:

> "including:
> • a foreign intelligence standard instead of a criminal standard of probable cause;
> • use of the most advanced and highly intrusive techniques for intelligence gathering; and
> • surveillances and searches for extensive periods of time;
> based on a standard that the U.S. person is only using or about to use the places to be surveilled and searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants."[11]

Judge Lamberth observed that the FISC's members had "specialized knowledge," had reviewed "several thousand FISA applications," and were "mindful of the FISA's preeminent role in preserving our national security, not only in the present national emergency, but for the long term as a constitutional

[11] *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 624 (For. Intel. Surv. Ct. 2002).

democracy under the rule of law."[12] It reasoned that, as a result, it retained supervisory powers to protect against the misuse of FISA for criminal investigative purposes.

The Foreign Intelligence Surveillance Court of Review reversed this opinion, reasoning that section 218 of the Patriot Act had stripped the FISC of this role.[13] If Congress reauthorizes section 218, it should amend it to make clear that, although the "wall" is no more, section 218 does not prohibit the FISC from adopting reasonable guidelines to prevent the direction and control of foreign intelligence investigations by prosecutors for law enforcement ends.

Surveillance under FISA is growing rapidly. As a result in part of section 218, the FISA statute, which is supposed to be directed at a narrow subset of national security investigations, is fast become the preferred method of government surveillance. In 2003 and 2004, for the first time in history, there were more surveillance orders issued by the FISA court than by every other court – state or federal – in the United States for criminal surveillance under Title III.

This shift in law from a more open criminal surveillance statute based on probable cause of crime, towards a more secret surveillance statute, not based on probable cause of crime, has serious implications for civil liberties. Congress should explore a remedy for one of the those problems: the lack of "adversarial discovery for FISA applications and warrants." This is in marked contrast to the extensive discovery available to criminal defendants, enabling the court to hold government officials accountable for unlawful searches and surveillance.

Congress should enact legislation making available to the defense such "adversarial discovery of FISA applications and warrants" using the carefully-crafted Classified Information Procedures Act (CIPA). The ACLU strongly supports H.R. 1502, the Civil Liberties Restoration Act (CLRA), sponsored by Representatives Howard Berman (D-CA) and John Conyers, Jr. (D-MI), which includes this provision at section 401.

*Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004.*
Section 6001 further eroded the basic safeguards included in FISA by authorizing, for the first time, secret searches and surveillance of homes and businesses where there is neither criminal probable cause nor probable case that the person is acting on behalf of any foreign power.

FISA rests what would otherwise plainly be unconstitutional searches (because they are not based on probable cause of crime) on an alternate showing: probable cause that those individuals are acting on behalf of a foreign power. By eliminating this alternate showing for non-citizen visitors to the United States suspected of being "lone wolf" terrorists, we believe section 6001 violates the Fourth Amendment.

---

[12] *Id.* at 615.
[13] *See In re Sealed Case*, 310 F.3d 717 (For. Intel. Surv. Ct. Rev. 2002).

Moreover, section 6001 was not needed to address deficiencies in the use of FISA search powers uncovered after September 11, its original rationale. The National Commission on Terrorist Attacks Upon the United States ("9-11 Commission") uncovered a number of serious, structural breakdowns in the intelligence community prior to September 11. A lack of legal authority to collect intelligence information was not among its findings.

Section 6001 has erroneously been described as necessary to respond to the government's failure to seek a warrant to search the laptop computer of suspected terrorist Zacarias Moussaoui. The 9-11 Commission rejected that conclusion, finding that government agents "misunderstood and misapplied" guidelines regarding FISA search warrants, and that these mistakes contributed to their failure to seek either a criminal or FISA warrant in the Moussaoui case.[14] The 9-11 Commission did not recommend any change to existing legal authorities, including FISA.

In a February 2003 report on FISA oversight, Senators Leahy, Grassley and Specter noted, with respect to this proposed change, that the Department of Justice was unable to provide even a single case, even in a classified setting, that explained why what became section 6001 was needed. As the report states, "In short, DOJ sought more power but was either unwilling or unable to provide an example as to why."

Section 6001 could do serious harm to the government's anti-terrorism efforts if a court concludes (as we believe it will) that the surveillance it authorizes violates the Fourth Amendment, making the evidence obtained by such surveillance inadmissible. The "foreign power" standard – which section 6001 eliminates for non-citizens – is integral to the rationale given by the Foreign Intelligence Surveillance Court of Review in its opinion upholding FISA surveillance against a constitutional challenge.[15]

This committee should review carefully actual applications for secret searches or surveillances under the new power provided by section 6001 to determine whether such searches or surveillance could have been undertaken using traditional criminal powers, and whether section 6001 "actually materially enhances security." If the government satisfies this test and Congress decides to re-authorize section 6001, Congress should consider additional safeguards.

When S. 113, the legislation that became section 6001, was being debated in the Senate, Senator Dianne Feinstein offered a compromise that the ACLU supported. The Feinstein amendment would have formally preserved the FISA requirement that the FISA court determines that the target of a surveillance order is an agent of a foreign power before a surveillance order is authorized, but it allowed the court to presume such agency. The amendment is problematic because it allows the court to presume agency based on conduct that does not

---

[14] *Final Report of the National Commission on Terrorist Attacks Upon the United States* 79, 540 n.94 (2004).

[15] See *In re Sealed Case*, supra, at 738 (relying on "foreign power" probable cause to hold that FISA secret searches and surveillance satisfy Fourth Amendment standards of reasonableness).

necessarily show such agency. Nevertheless, because the amendment would preserve some discretion on the part of the FISA court to determine that an individual should not be subject to surveillance because they are not, in fact, an agent of a foreign power, the ACLU urges Congress to adopt the Feinstein amendment if it decides to reauthorize section 6001.

## Wiretapping and Electronic Surveillance Without Judicial Safeguards Limiting Orders to the Targets of an Investigation

"General warrants" – blank warrants that do not describe what may be searched – were among those oppressive powers used by the British crown that led directly to the American Revolution. As a result, the framers required all warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized."

The same "particularity" requirements apply to wiretap orders. In the landmark case *United States* v. *Donovan*, 429 U.S. 413 (1977), a majority upheld the federal criminal wiretap law, noting that Congress had redrafted the law to include safeguards regarding, among other things, the need to identify targets of surveillance in response to the "constitutional command of particularization."[16]

*Section 206 of the Patriot Act.* Section 206 erodes the basic constitutional rule of particularization by creating "roving wiretaps" in foreign intelligence cases without sensible privacy safeguards. As amended by later legislation, these wiretaps do more than allow the government to get a single order that follows the target of surveillance from telephone to telephone. The government can now issue "John Doe" roving wiretaps that fail to specify a target or a telephone, and can use wiretaps without checking that the conversations they are intercepting actually involve a target of the investigation. Section 206 is subject to the Patriot Act's sunset clause.

Prior to the passage of the Patriot Act, roving wiretaps were available in criminal investigations (including criminal investigations of terrorists), but were not available in foreign intelligence investigations.

Because roving wiretaps contain more potential for abuse than traditional wiretaps, which apply to a single telephone or other device, when Congress enacted roving wiretaps for criminal investigations, it insisted on important privacy safeguards.

First, a criminal wiretap must specify either the identity of the target or the communications device being used. In other words, a surveillance order may specify only the target, or only the phone, but it must specify one or the other. Second, a criminal wiretap that jumps from phone to phone or other device may not be used unless the government "ascertains" that the target identified by the order is actually using that device.

[16] *Id.* at 426-27 (quoting S. Rep. No. 1097, 90th Cong., 2nd Sess., at 66 (1968), *reprinted in* U.S. Code Cong. and Admin. News 1968, at 2190).

When Congress enacted the Patriot Act, it extended "roving wiretap" authority to FISA investigations, but did not include the common sense "ascertainment" safeguard. Shortly thereafter, the newly enacted roving wiretap authority was broadened by the Intelligence Act for FY 2002, which authorized wiretaps where neither the target nor the device was specified. As a result, FISA now allows "John Doe" roving wiretaps. These are new wiretaps that can follow an unknown suspect from telephone to telephone based only on a potentially vague physical description.

The Justice Department points to the need to provide a physical description, and the need to show "probable cause" that the wiretap will intercept conversations of an agent of a foreign power, as sufficient protection for roving surveillance. Congress provided more exacting scrutiny for criminal roving wiretaps, and it should provide additional safeguards here. A roving tap, unbounded by any need to identify the target, opens the door to surveillance of anyone who fits that description, or (because of the lack of an ascertainment requirement) anyone else who might be using that telephone.

Of course, particularization is a separate constitutional demand; probable cause does not satisfy the Fourth Amendment without particularization. For that reason, the criminal roving wiretap statute includes the requirement to identify a target even though criminal wiretap orders also require criminal probable cause. FISA wiretaps, of course, require no probable cause of crime, so the need for safeguards is, if anything, greater.

In its defense of section 206 of the Patriot Act, the Justice Department takes issue with both the ascertainment requirement and the requirement to identify the target of a roving wiretap. The Justice Department's "sunsets report" implies, wrongly, that the ascertainment requirement only applies to oral interceptions (i.e., bugs) and not to wiretaps. [17] While the wording of the ascertainment requirement for wiretaps is different than the same requirement for oral interception,[18] there is no doubt that the criminal wiretap statute bans "John Doe" roving wiretaps and requires ascertainment.

18 U.S.C. § 2518(11)(b), which applies to wire and electronic communication, plainly provides that no judge may issue a roving wiretap unless, among other things:

> the application identifies the person believed to be committing the offense and whose communications are to be intercepted and . . . the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

[17] Department of Justice, *USA PATRIOT Act: Sunsets Report* (April 2005), at 20.
[18] *See* 18 U.S.C. § 2518(12) (ascertainment requirement for oral interception).

Congress should tighten the FISA roving wiretap so that it has the sensible safeguards for privacy, just as criminal roving wiretaps. Indeed, FISA roving wiretaps appear to be far more common than criminal roving wiretaps. Attorney General Gonzales reported in testimony before the House Judiciary Committee on April 6, 2005 that FISA roving wiretaps had been issued 49 times since passage of the Patriot Act. By contrast, the federal government reported only one federal criminal roving wiretaps in 2004, with twelve criminal roving wiretaps in the entire 2002-2004 period.[19]

Supporters of the Patriot Act often argue that changes to the law were needed to give the government the same powers in foreign intelligence investigations that it already had in criminal investigations. To the extent that is appropriate, it is fair to insist that the same safeguards apply as well.

Section 2 of H.R. 1526, the SAFE Act, would provide just such safeguards. While it preserves FISA roving surveillance authority, it also makes sure that these privacy safeguards, which apply to criminal roving wiretaps, would also apply to FISA roving wiretaps.

*Section 207 of the Patriot Act.* The time periods for foreign intelligence surveillance orders were already much longer than for criminal surveillance orders even before the passage of the Patriot Act. Permitting surveillance to continue for a year with no judicial review opens the door for abuse. The Justice Department's main justification for allowing review to continue for such a long period has been the ability to conserve attorney time and other resources needed to process renewal applications.

If the administration can show the sharp increases in FISA secret searches and surveillance enabled by this and other provisions "actually materially enhances security," Congress should consider the cost in lost oversight of highly intrusive powers. It may be possible to get the benefits while preserving oversight.

Congress should consider whether it can shorten these periods by conducting a searching review of FISA surveillance conducted under the lengthened periods. Was it productive for the entire period it was authorized? If the problem is a lack of resources, the solution should not be to shortchange judicial oversight. Precisely because there is increased pressure to engage in surveillance early to prevent terrorism before it happens, there is an increased danger of abuse and an increased need for judicial oversight. Congress should provide sufficient funds both to the Department of Justice and to the Foreign Intelligence Surveillance Court to handle the important work of reviewing surveillance orders.

## Internet Surveillance without Probable Cause: Web Browsers, E-Mail, and "Pen/Trap" Devices

[19] Wiretap reports are available at the website of the Administrative Office of the U.S. Courts, at http://www.uscourts.gov/library/wiretap.html

While the "probable cause" standard has long applied both to physical searches and electronic intercepts of the content of conversations, surveillance techniques that monitor only who is sending or receiving information (often called "routing information"), but do not intercept the content of communications, do not require probable cause.

For telephones, pen registers and "trap and trace" devices have long been available to track the telephone numbers dialed, and the telephone numbers of incoming calls. These numbers could then be cross-referenced, through a reverse telephone directory, to identify to whom a target of a pen/trap device is calling. A similar technique, "mail covers," is used to track the outside cover of an envelope sent through the mail. Neither technique requires probable cause, although a court order may be needed.

Prior to the passage of the Patriot Act, it was unclear how the law allowing pen/trap devices for telephone communications applied to communications over the Internet. Federal agents argued they should be allowed, without showing probable cause or obtaining a surveillance order, to monitor the "header" information of an e-mail and the URL of a web page.

Privacy advocates urged caution, noting that Internet communications operate very differently than traditional mail or telephone communications. For example, the "header" information of an e-mail contains a wealth of information, such as a subject line or an entire list of thousands or even hundreds of thousands of addressees. A monitoring order would allow the government to obtain, without probable cause, a political, charitable or religious organization's electronic mailing list. In short, e-mail headers provide far more content than is typical on the outside of an envelope.

Likewise, the "link" at the top of a web browser contains not only the website visited, but also the precise pages viewed, or the search terms or other information entered by the user on a web-based form. For example, in the popular search engine "google," a user looking for information about a drug such as "viagra" generates the web address http://www.google.com/search?hl=en&lr=&q=viagra.

Section 214 of the Patriot Act broadens the use of Internet surveillance, without probable cause, by extending the pen/trap surveillance technique from a relatively narrow arena of facilities used by agents of foreign powers or those involved in international terrorism to include any facility. Pen/trap surveillance can now be used far more widely to monitor the Internet use of ordinary Americans.

Pen/trap for the Internet suffers from a basic flaw: in extending this intrusive surveillance authority to the Internet, Congress did not adequately take account the differences between the Internet and traditional communications that make intercept of Internet "routing information" far more intrusive as applied to Internet communications.

If the administration can show that section 214 of the Patriot Act "actually materially enhances security" and should be renewed, Congress should insist on additional protections to take into account the differences between Internet and traditional telecommunications.

Congress should insist on rules that:

- Clearly define content for Internet communications. Congress should be specific. For e-mails, at the very least, the subject line and any private (i.e., "bcc") list of addresses should be off limits without a surveillance order based on probable cause. For Internet browsing, obtaining any information behind the top level domain name should likewise be barred without probable cause. For example, an agent could obtain a list of websites visited (like www.aclu.org) but not of webpages visited (like www.aclu.org/patriotact ) or search terms entered (like http://www.google.com/search?hl=en&q=aclu+craig+durbin+safe+act ).

- Prevent techniques that acquire content from being used in the absence of an order based on probable cause. The Internet does not work like traditional telephones or the mail. The constitutionally protected content of communications may be difficult, or even impossible, to separate from the "routing information." For example, e-mail may be sent through the Internet in discrete "packets," rather than as a single file, to permit the information to be sent along the most efficient route, then reassembled at the destination, using codes that are attached to the packets of information. The burden should be on the government to develop techniques that do not incidentally acquire content. In the absence of those techniques, a surveillance order based on probable cause should be required. Federal agents should not be put in the untenable position of incidentally gathering constitutionally-protected content in the course of obtaining "routing information," and then being forced to delete or ignore the content information.

The debate over extending pen/trap authority, which is not based on probable cause, to Internet communications, is not about whether criminals or terrorists use the Internet. Of course they do. The question is how to ensure that Congress does not erode the privacy of everyone by authorizing surveillance techniques, not based on probable cause, that fail to account for the differences between traditional communications and Internet communications.

Because pen/trap authority as applied to the Internet is particularly intrusive, even with rules that define content more properly, Congress should insist that pen/trap orders require more specific justification. The ACLU urges adoption of a provision in the Senate version of the SAFE Act. Section 6(b) of S. 737 would require, for FISA pen/trap authority, more than a simple certification that the information is relevant to a foreign intelligence investigation.

While S. 737 would not require probable cause for FISA pen/trap authority it adds teeth to the relevance test. S. 737 would require the government to provide

a "statement by the applicant of specific and articulable facts showing there is reason to believe" the information obtained by the pen/trap device is relevant to the investigation.

*Conclusion: Restoring Checks and Balances*

The Patriot Act provisions that pose the greatest challenges share certain common themes. As a result of gag orders, or delayed notification, they permit surveillance with a far greater degree of secrecy than is common in most government investigations. They do not allow affected parties the opportunity to challenge government orders before a judge. Finally, because the substantive standards for some forms of surveillance have been modified, weakened, or even eliminated, the role of the Foreign Intelligence Surveillance Court in checking government abuse has been made less meaningful.

This committee's review of the Patriot Act and related legal measures in the ongoing effort to combat terrorism is needed to ensure continued public support for the government's efforts to safeguard national security. The controversy over the Patriot Act reflects the concerns of millions of Americans for preserving our fundamental freedoms while safeguarding national security.

Patriot Act resolutions have been passed in 379 communities in 43 states, including six state-wide resolutions. These communities represent approximately 57 million people who oppose some intrusive sections of the Patriot Act and are calling for reform. The resolutions have passed in strongly conservative states, such as Idaho and Alaska, as well as progressive states like Vermont. A nationwide coalition under the banner "Patriots to Restore Checks and Balances" has formed under the leadership of former Congressman Bob Barr (R-GA), and includes groups as diverse as the ACLU, the American Conservative Union, the Free Congress Foundation, and Gun Owners of America.

Such widespread concern, across ideological lines, reflects the strong belief of Americans that security and liberty need not be competing values. Congress included a "sunset provision" precisely because of the dangers represented by passing such far-reaching changes in American law in the aftermath of the worst terrorist attack in American history. Now is the time for Congress to complete the work it began when it passed the Patriot Act, by bringing the Patriot Act back in line with the Constitution.

## Example of Patriot Act Abuse

## Brandon Mayfield

On March 11, 2004 a bomb exploded in Madrid killing hundreds of people. The government obtained from Spanish authorities fingerprint images from a blue bag found at the scene containing seven detonators thought to be of the same type used in the bombing. The FBI concluded that the fingerprints matched those of a Portland attorney, Brandon Mayfield. He was arrested on May 6 on a material witness warrant.

Court documents show that Brandon Mayfield, a convert to Islam, was investigated at least in part because of his religion. For example, the material witness warrant alleged, among other things, that Mayfield, a Muslim, was seen driving from his home to the Bilal mosque, where he worshipped.

On March 24, 2005, the FBI admitted to Mayfield's attorney that his home had been secretly searched under the Foreign Intelligence Surveillance Act (FISA), which the Patriot Act amended. The FBI admitted that it copied four computer hard drives, digitally photographed several documents, seized ten DNA samples and took approximately 335 digital photographs of the residence and Mr. Mayfield's property. At an April 5 hearing before the Senate Judiciary Committee, Attorney General Gonzales specified that Sections 207 and 218 of the Patriot Act had been used. Section 207 lengthened the allowable time allotted to the FBI to secretly search Mayfield's home. Section 218 makes it easier to use intelligence authorities in criminal cases.

The Patriot Act facilitated FISA search of Mayfield's home. Before the law's passage, the government could conduct a FISA search only if the "primary purpose" of the search was to gather foreign intelligence information. Under Section 218 of the Patriot Act, gathering such information need only be a "significant purpose" of a FISA search. The Mayfield search occurred directly after the Madrid bombing as part of the FBI's investigation. This suggests strongly that the "primary purpose" of the search was not to gather foreign intelligence information, but to uncover incriminating evidence.

Prior to the Patriot Act, authorities would not have been able to use FISA to conduct absolutely secret "black bag" intelligence searches where the primary purpose of the search was criminal investigation. Instead, it is likely the government would instead have used a criminal search warrant, based on the more exacting standard of criminal probable cause. As a result, the government would have been forced to scrutinize its evidence more carefully, and could have caught its mistake long before it jailed an innocent man without charge for two weeks and labeled him a suspect in one of the most horrific terrorist attacks since September 11.

## Example of Patriot Act Abuse

## Unconstitutional National Security Letters

Section 505 of the Patriot Act expanded the government's authority to use National Security Letters (NSL's) to seize information from businesses and others, with no judicial approval. Prior to the Patriot Act, the government could use NSL's to obtain records about alleged terrorists or spies – people who were thought to be "foreign powers" or their agents. Financial, travel and certain Internet Service Provider (ISP) records are accessible under the NSL authority. Section 505 changed the law to allow the use of NSL's to obtain such records about anyone without the limitation that they be agents of foreign powers. In the Intelligence Authorization Act of 2004[20] Congress further expanded the NSL letter authority to permit seizure of casino and other records.

On a date that the government maintains must be kept secret for reasons of national security, the FBI served an NSL on an ISP the identity of which the government also claims must be kept secret for reasons of national security. Through its NSL authority at 18 U.S.C. Section 2709, the government can seek certain sensitive customer records from ISPs – including information that may be protected by the First Amendment – but the ISP can never reveal that it has been served with an NSL, and nothing in the statute suggests that the NSL can be challenged in court. On behalf of the ISP and itself, the ACLU challenged the statute as amended by the Patriot Act, as a violation of the First and Fourth Amendments because it does not impose adequate safeguards on the FBI's authority to force disclosure of sensitive and constitutionally protected information and because its gag provision prohibits anyone who receives an NSL from disclosing in perpetuity and to any person even the mere fact that the FBI has sought information.

On September 28, 2004, Judge Victor Marrero of the Southern District of New York issued a landmark decision striking down as unconstitutional the NSL statute and its gag provision. The court struck down the entire statute as violative of Fourth and First Amendment rights, thus rendering any use of the statute an abuse of those rights. The court found that there have been hundreds of such uses.[21] It found that the statute was abusive in practice because it sanctioned NSL's that coerced immediate compliance without effective access to court review or an opportunity to consult with counsel:

---

[20] Pub. L. No. 108-177, Section 374 (Dec. 13, 2003).

[21] *Doe v. Ashcroft*, (04 Civ. 2614, S.D.N.Y. Sept. 28, 2004), at 63-64. The court concluded that hundreds of NSL's had been requested by the FBI from October, 2001 through January, 2003, and hundreds must have been issued during the life of the statute. The government takes the position that even the number of NSL's it issues cannot be disclosed for reasons of national security, though it has disclosed publicly to Congress a number of such uses. *See, e.g.* "H.R. 3179, The 'Anti-Terrorism Intelligence Tools Improvement Act of 2003," Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 108th Cong. (2004) (statement of Thomas J. Harrington, Deputy Assistant Director of the FBI Counterterrorism Division).

> The form language of the NSL served upon [plaintiff ISP] Doe, preceded by an FBI phone call, directed him to personally provide the information to the FBI, prohibited him, his officers, agents and employees from disclosing the existence of the NSL to anyone, and made no mention of the availability of judicial review to quash or otherwise modify the NSL or the secrecy mandated by the letter. Nor did the FBI inform Doe personally that such judicial review of the issuance of the NSL or the secrecy attaching to it was available. The court concludes that, when combined, these provisions and practices essentially force the reasonable NSL recipient to immediately comply with the request.[22]

In finding the statute unconstitutional under the *Fourth* Amendment, Judge Marrero referred repeatedly to the amendments made by Section 505. He noted as an example of the kind of abuse now authorized by the statute that it could be used to issue a NSL to obtain the name of a person who has posted a blog critical of the government, or to obtain a list of the people who have e-mail accounts with a given political organization.[23] The government could not have obtained this information with an NSL prior to the Patriot Act amendment in Section 505, unless the blogger or the people with such accounts were thought to be foreign powers or agents of foreign powers. The court also cited Patriot Act Section 505 as a reason it struck down the statute on *First* Amendment grounds. The court determined that the tie to foreign powers – eliminated by Section 505 – "limits the potential abuse" of the statute[24] and distinguishes it from other intelligence search provisions that retain the requirement of such a tie and include a statutory gag provision.

Because of the gag in 18 U.S.C. Section 2709(c), the government obtained a sealing order it has consistently used to suppress wholly innocuous information in the litigation. Until the court struck down the statute, the government prevented the ACLU from disclosing that it represented someone that had been served with an NSL, and from even acknowledging that the government had used a statutory power. The government has demanded that the ACLU redact a sentence that described its anonymous client's business as "providing clients with the ability to access the Internet." Ironically, the government even insisted that the ACLU black out a direct quote from a Supreme Court case in an ACLU brief: "The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent."

The gag in Section 2709 would effectively prevent an ISP (or its lawyers) from disclosing other abuses of Section 2709. For example, if the government was targeting someone because of their First Amendment activity, or if the ISP was being forced to turn over First Amendment protected information about associational activities, the gag would bar disclosure of this abuse.

---

[22] *Id*. at pp. 44-45.
[23] *Id.* at p. 75.
[24] *Id*. at p. 93.

## Examples of the Chilling Effects of Patriot Act Section 215

In July 2003, the ACLU filed suit on behalf of six community and non-profit organizations because it had learned of a serious chilling effect that resulted from Section 215 of the Patriot Act.[25] Excerpts from some plaintiffs' declarations highlight how Section 215 chills political speech and hinder privacy rights:

**The president of a community association:** "The enactment of Section 215 has significantly changed the way members of [the Muslim Community Association of Ann Arbor, or MCA] participate in the organization. Many previously active members have become passive ones. Attendance at daily prayer services, educational forums, and social events has dropped. Some members have totally withdrawn their membership from MCA. Charitable donations to MCA have decreased."[26]

**A prominent member of the association:** "Although I had been very outspoken politically before passage of the Patriot Act, I became afraid after the Patriot Act was passed that if I continued to remain a vocal and visible Muslim, the government would target me for investigation and seek private records about me even thought I had not done anything wrong.

"While I was upset by several policies of the U.S. and would have ordinarily taken a leadership role in protesting these policies, I decided to step out of the limelight to lessen the chances that the government would target me for an investigation under the Patriot Act."[27]

**The administrator of a Christian refugee aid organization:** "Section 215 has harmed our ability to serve our clients in a number of different ways.

"Section 215 has caused Bridge to redirect resources from client assistance. Resources that we otherwise would have used to help clients are instead being used to re-evaluate our record-keeping and record retention policies.

"Because we would not have an opportunity to challenge a Section 215 order before complying with it, we have had no choice but to act now to ensure that our records do not contain personal or other sensitive information that we could be forced to disclose to the government. Accordingly, my staff and I have been deciding on a case-by-case basis to exclude some sensitive information from our files.

"While we believe that we have no practical choice but to adopt this policy, there is no question that the practice compromises the level of services we can provide to our clients."[28]

---

[25] *Muslim Community Association of Ann Arbor v. Ashcroft*, Civil Action No. 03-72913 (E.D. Mich., filed July 30, 2003).
[26] Nazih Hassan Decl. ¶ 22.
[27] John Doe (Member of MCA) Decl. ¶¶ 8-9.
[28] Mary Lieberman Decl. ¶¶ 23-27.

# Patriot Act Intelligence Authorities: Recommended Safeguards

| *Intelligence Surveillance power* | *Before 9/11* | *Now* | *Sunsets?* | *Recommended safeguard (if power is retained)* |
|---|---|---|---|---|
| FISA records search orders<br>**-Patriot Act § 215** | FISA search orders were available only for certain travel-related "business" records on basis of individualized suspicion connecting records to foreign agent. | Now these orders are available for any and all "tangible things," including library records, medical records, and other highly personal records, without individual suspicion. | Yes | Congress should enact legislation limiting such orders to where the FBI has "specific and articulable facts" connecting records to foreign agent.<br>**-SAFE § 4 (H.R. 1526)**<br>In addition, Congress should provide a right to challenge the order, limits on the secrecy order and a right to challenge that order, and notice and an opportunity to challenge the use of such information in court.<br>**-SAFE § 4 (S. 737)** |
| National security letters (no court order required) for financial records, telephone and ISP bills, consumer credit reports.<br>**-Patriot Act § 505**<br>**-Intelligence Act for FY2004 § 334** | Were available only where FBI could show "specific and articulable facts" connecting records to foreign agent. | Now available without individual suspicion; definition of "financial records" greatly expanded. | No | Congress should enact legislation that restores the requirement of individual suspicion, provides a right to challenge records demands, limits the secrecy order and provides for a right to challenge the secrecy order, and providing notice to persons when the government seeks to use information from such demands against them in court.<br>**-SAFE § 5 (S. 737)** |
| FISA secret searches and wiretaps in criminal investigations<br>**-Patriot Act § 218** | Available only if "primary purpose" is to obtain foreign intelligence | Permitted when "primary purpose" is criminal investigation, as long as "a significant purpose" is foreign intelligence | Yes | Congress should clarify that FISC retains supervisory power to ensure FISA searches are not directed or controlled by criminal prosecutors<br>**-codify In re All Matters, 218 F. Supp. 2d 611 (FISC 2002)**<br>Congress should enact legislation to give the defense access to FISA applications and warrants, subject to the national security protections in the Classified Information Procedures Act<br>**-Civil Liberties Restoration Act, H.R. 1502 § 401** |

| *Intelligence Surveillance power* | *Before 9/11* | *Now* | *Sunsets?* | *Recommended safeguard (if power is retained)* |
|---|---|---|---|---|
| Extended duration of FISA secret searches and wiretaps<br>**-Patriot Act § 207** | Electronic surveillance orders for 90 days, renewal for 90 days; physical search orders last for 45 days | Initial electronic surveillance for 6 months, renewals for one year; physical search orders last 90 days for US persons and 6 months for foreign visitors and temporary residents | Yes | Congress should extend the sunset of this provision and investigate whether shorter time periods to ensure continued court oversight are appropriate, and should increase appropriations to Justice Department and FISC to provide sufficient resources to process applications. |
| FISA secret searches and wiretaps without connection to foreign power<br>**-Intelligence Reform Act of 2004 § 6001** | All secret search and surveillance orders required probable cause of connection to foreign power | For non-US persons, FISA secret search or surveillance allowed for persons "involved in international terrorism" or "preparations therefore" without any foreign power connection | Yes | Congress should allow the FISC to presume that a non-US person involved in international terrorism is acting for a foreign government or organization, but should not make such a presumption mandatory or eliminate altogether the "foreign power" requirement<br>**-Feinstein Amdt. to S. 113 (108th Cong.)** |
| FISA roving wiretaps<br>**-Patriot Act § 206**<br>**-Intelligence Act for FY2002 § 314.** | No roving wiretaps under FISA, but were available for criminal investigations | Now there are FISA roving wiretaps, but unlike criminal roving wiretaps, FISA roving wiretaps do not need to specify target and agents need not ascertain target is using that telephone. | Yes | Congress should enact legislation that would require FISA roving wiretaps to observe same requirements as criminal roving wiretaps, i.e., they must (1) specify a target, and (2) would have to ascertain target is using that facility.<br>**-SAFE Act § 2 (H.R. 1526)** |
| FISA surveillance of the Internet, other communications without probable cause with pen/trap authority<br>**-Patriot Act § 214** | Available only for facilities used by agents of foreign power or those involved in international terrorism activities | Can be used for more broadly, including for U.S. persons, and regardless of what facility is being monitored | Yes | Congress should require rules that define content for the Internet more clearly and prohibit techniques that acquire content without probable cause.<br>-(no legislative language)<br>Congress should require determination of relevance to be based on a statement of "specific and articulable facts," not on mere certification<br>**-SAFE Act § 6 (S. 737)** |