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 an Oversight Hearing on

sections 206 and 215 of the

USA PATRIOT Act of 2001

Before the

Subcommittee on Crime, Terrorism and Homeland Security

of the

House Judiciary Committee

Submitted by

Gregory T. Nojeim
Associate Director and Chief Legislative Counsel
Washington Legislative Office

and

Timothy H. Edgar
National Security Policy Counsel

April 28, 2005

American Civil Liberties Union
Testimony at an Oversight Hearing on sections 206 and 215
of the USA PATRIOT Act of 2001
before the Subcommittee on Crime, Terrorism and Homeland Security
of the House Judiciary Committee
Submitted by Gregory T. Nojeim,
Associate Director and Chief Legislative Counsel,
and Timothy H. Edgar, National Security Policy Counsel

April 28, 2005

Chairman Coble and Ranking Member Scott:

It is a pleasure to testify before you on behalf of the American Civil Liberties Union at this oversight hearing on two sections of the USA Patriot Act – section 215, a provision allowing the government to obtain library, bookstore and other personal records in foreign intelligence cases without individual suspicion, and section 206, the provision authorizing roving wiretaps in foreign intelligence cases.

The Patriot Act became law only 45 days after the September 11 attacks. While it acted swiftly, Congress subjected approximately a dozen provisions of the Patriot Act to a sunset date of December 31, 2005, so that it could take a second look at 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.

Congress should use the 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 power, this committee should require the Executive Branch to meet the standard articulated by the bipartisan 9-11 Commission.

- First, Congress should take care not to renew any provision unless the government can show "(a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties."[1]

- Second, "[i]f the power is granted, there must be adequate guidelines and oversight to properly confine its use."[2]

- Finally, Congress should resist efforts by the Executive Branch to evade searching review of its existing powers, both under the Patriot Act and under other legal authorities, by

[1] Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission Report") 294-95 (2004) (boldfaced recommendation)
[2] *Id.*

shifting the debate to new anti-terrorism legislation, such as proposals for administrative subpoenas.

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.

Section 215: Power to Obtain Library and Bookstore Records, Medical Records, Other Personal Information and "Tangible Things" Outside a Criminal Investigation

Section 215 of the Patriot Act expanded the Foreign Intelligence Surveillance Act to authorize the FBI to more easily obtain a court order requiring a person or business to turn over documents or things "sought for" an investigation to protect against international terrorism or clandestine intelligence activities.

Section 215 is not the only newly expanded records-gathering power within the Patriot Act, although it is the only such power subject to the sunset clause. Section 505 of the Patriot Act expanded national security letter authority to allow the FBI to issue a letter compelling Internet Service Providers, financial institutions and consumer credit reporting agencies to produce records about people who use or benefit from their services. This power was later expanded to include records of car dealers, boat dealers, jewelers, real estate professionals, pawnbrokers and others. Because section 505 raises many of the same concerns as section 215 without even the requirement of a FISA court order, Congress should examine section 505 at the same time as it examines section 215.

For both section 215 records searches and national security letters, the Patriot Act removed from the law the requirement that the records being produced pertain to an "agent of a foreign power," – that is, foreign countries, businesses, and terrorist organizations. This significantly expanded law enforcement access to records pertaining to Americans. In these days of data mining, one cannot ignore this stark fact: under these provisions, the government can easily obtain records pertaining to thousands of Americans who have nothing to do with terrorism, so long as the records are sought for, or are allegedly relevant to, one of these investigations.

Both powers differ markedly from traditional criminal subpoenas. Neither of these statutes signals the recipient of a letter or order that the recipient can challenge it in court. Both statutes indicate that the recipient can tell no one that the recipient has received the order or letter, including any attorney with whom they may like to consult. In common parlance, recipient is "gagged," and under the statutory language, the gag stays in place forever.

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 First and Fourth Amendment grounds. As explained in

the case example (attachment A), 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, described in further detail in attachment B, 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.[3]

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 could be used to obtain a list of the books or magazines someone purchases or borrows from the library. A FISA record demand could 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.

[3] 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.

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 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.[4]

Congress should not accept the superficial argument that every power that is available in a criminal investigation should be available to the same extent in a foreign intelligence investigation. Grand juries have extraordinary powers to compel documents and testimony for investigative purposes that would be entirely inappropriate in the hands of intelligence agents.

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.

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

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.[5]

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 involve an "agent of a foreign power" for FISA records demands and provides a sunset date for the expanded national security letter power.[6] 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 be marked up in this subcommittee or in the full Judiciary Committee.[7] 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.

<u>"Roving Wiretaps" Without Sensible Privacy Safeguards</u>

"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."[8]

---

[5] 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.

[6] A section-by-section chart of H.R. 1526 is appended as attachment C.

[7] A section-by-section chart of S. 737 is appended as attachment D.

[8] *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).

Section 206 of the Patriot Act 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.

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. [9] While the wording of the ascertainment requirement for wiretaps is different than the same requirement for oral interception,[10] 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.

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 six federal criminal roving wiretaps in 2003 (the latest report available), with nine federal criminal roving wiretaps in 2002.[11]

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.

Conclusion

In short, we are not asking that law enforcement tools be taken away. Rather, that they be made subject to reasonable checks and balances – such as meaningful judicial oversight and appropriate disclosure to the public of use of the power.

Congress could easily make some of the needed reforms to sections 206 and 215, as well as other important reforms, by adopting the Security and Freedom Ensured Act, or SAFE Act, H.R. 1526.

---

[9] Department of Justice, *USA PATRIOT Act: Sunsets Report* (April 2005), at 20.
[10] *See* 18 U.S.C. § 2518(12) (ascertainment requirement for oral interception).
[11] Wiretap reports are available at the website of the Administrative Office of the U.S. Courts, at http://www.uscourts.gov/library/wiretap.html

This bipartisan legislation is co-sponsored by, among others, Representatives Otter (R-ID), Flake (R-AZ), Sanders (I-VT) and Conyers (D-MI). Its Senate counterpart, the Security and Freedom Enhancement Act, S. 737, is sponsored by Senators Craig (R-ID) and Durbin (D-IL).[12]

Adopting the SAFE Act would go a long way toward bringing it more into line with the Constitution, and advancing the goal of keeping America both safe and free.

[12] See attached charts explaining H.R. 1526 and S. 737.

Attachment A: 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.[13] 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."[14]

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."[15]

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."[16]

---

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

Attachment B: 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[17] 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.[18] 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:

> 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

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

[18] *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).

> available. The court concludes that, when combined, these provisions and practices essentially force the reasonable NSL recipient to immediately comply with the request.[19]

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.[20] 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[21] 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.

---

[19] *Id*. at pp. 44-45.
[20] *Id*. at p. 75.
[21] *Id*. at p. 93.

Attachment C: Section-by-Section of H.R. 1526: Security and Freedom Ensured (SAFE) Act Providing Checks and Balances for Patriot Act Surveillance Powers

surveillance power	*before Patriot Act*	*now*	*SAFE Act safeguard*
Roving wiretaps under the Foreign Intelligence Surveillance Act (FISA).		✓	✓
	No roving wiretaps under FISA, but were available for criminal investigations (including for terrorism). Criminal roving taps require that target of search is specified and agents "ascertain" that target is using the facility.	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. **PATRIOT § 206; Intelligence Act for FY2002 § 314.**	Would keep FISA roving wiretaps, but they would have 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. **SAFE § 2**
"Sneak and peek" – criminal search warrants with delayed notice.	✓	✓	✓
	Some courts had approved in specific circumstances, despite lack of statutory authority. Two circuit courts of appeals imposed presumptive seven-day limit on delaying notice.	Now there is statutory authority for sneak and peek searches under wide-ranging circumstances, including whenever notice could "seriously jeopardize" a prosecution or delay a trial. No time limit for delaying notice **PATRIOT § 213**	Would limit statutory reasons for delaying notice to four specific harms – danger to persons, flight from prosecution, intimidation of a witness, or destruction of evidence – and imposes a seven-day limit, which court can renew for periods of (21 days?) **SAFE § 3**
Library and other personal records searches under FISA.		✓	✓
	FISA search orders were available only for certain travel-related "business" records (not library or personal records) where FBI has "specific and articulable facts" connecting records to foreign agent.	Now these orders are available for any and all records, including library records, without individual suspicion. **PATRIOT § 215**	Would still be available for any and all records – including library records – but only where FBI has "specific and articulable facts" connecting records to foreign agent. **SAFE § 4**

surveillance power	*before 9/11*	*now*	*after SAFE*
National security letters (no court order required) for financial records, telephone and ISP records, consumer credit reports.	✓	✓	✓
	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. **PATRIOT § 505; Intelligence Act for FY2004 § 334.**	Would still be available without individual suspicion, but libraries with Internet terminals would not be subject to national security letters. **SAFE § 5**
Definition of "Domestic Terrorism"		✓	✓
	none	any state or federal criminal act involving "acts dangerous to human life" and intending to influence government or civilian population **PATRIOT § 802**	any act involving a listed federal crime of terrorism intending to influence government or civilian population **SAFE § 6**
Sunset clause.	not applicable	Now applies to 14 provisions (out of 158 total). **PATRIOT § 224**	Would be expanded to include four additional provisions, for a total of 18 (out of 158 total). **SAFE § 7**

Attachment D: Section-by-Section of S. 737: Security and Freedom Enhancement (SAFE) Act Providing Checks and Balances for Patriot Act Surveillance Powers

	Surveillance power	*Before Patriot Act*	*Now*	*Sun-sets?*	*SAFE Act safeguard*
1	Short title.				
2	Foreign intelligence (FISA) roving wiretaps. **-Patriot Act § 206 -Intelligence Act for FY2002 § 314.**	No roving wiretaps under FISA, but were available for criminal investigations, including criminal terrorism investigations.	FISA roving wiretaps allowed in all intelligence investigations, 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	The SAFE Act would retain roving wiretaps in FISA investigations, but 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.
3	"Sneak and peek" searches -- criminal search warrants with delayed notification. **-Patriot Act § 213**	Some courts had approved in specific circumstances, despite lack of statutory authority. Two circuit courts of appeals imposed presumptive seven-day limit on delaying notice.	Patriot Act provides statutory authority for sneak and peek searches under wide-ranging circumstances, including whenever notice could "seriously jeopardize" a prosecution. No time limit for delaying notice.	No	The SAFE Act would limit statutory reasons for delaying notice to specific harms – danger to persons, flight from prosecution, destruction of evidence, or intimidation of witnesses – and imposes a seven-day limit, which court can renew for additional periods of 21 days.
4	FISA records search orders **-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	The SAFE Act allows orders for all "tangible things," including library records. It limits all orders to where the FBI has "specific and articulable facts" connecting records to foreign agent. In addition, it provides 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.

5	National security letters (no court order required) for financial records, telephone and ISP bills, consumer credit reports. **-Patriot Act § 505 -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	The SAFE Act retains the broader definition of "financing records." It 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.
6	Surveillance of the Internet, other communications without probable cause using pen/trap authority. **-Patriot Act §§ 214 (criminal) and 216 (FISA)**	Unclear whether pen/trap authority applied to the Internet; FISA pen/traps available only for facilities used by agents of foreign power or those involved in international terrorism activities.	Pen/trap authority extended to Internet communications; FISA pen/traps can be used at more facilities, including for U.S. persons, and regardless of what facility is being monitored.	Yes-(214) No-(216)	The SAFE Act would require that the determination of relevance for pen/trap orders (both FISA and criminal) be based on a statement of "specific and articulable facts," not on mere certification. It requires more detailed reporting for criminal pen/trap devices (including reporting on what information is obtained) and notice when surveillance is terminated. **-SAFE Act § 6**
7	Definition of domestic terrorism, triggers other surveillance powers. **–Patriot Act § 802**	Definition of international terrorism only.	Domestic terrorism is <u>any</u> state or federal criminal act primarily within US involving "acts dangerous to human life" and that "appears to be intended" to influence government or civilian population.	No	The SAFE Act limits the definition to criminal acts involving a specific list of serious federal crimes of terrorism that are actually intended to influence government or civilian population.
8	Public reporting on FISA surveillance.	Only reporting is the yearly number of applications and number of orders granted.	Public reporting is unchanged. FISA was expanded by Patriot Act and is now used far more often. Section 6001 of the Intelligence Reform Act added new reporting requirements for Congress.	N/a	The SAFE Act expands sunshine by making public reporting under the 2004 intelligence reform act, which (1) breaks total number of FISA orders down into types of surveillance (wiretaps, physical searches, pen/trap, records searches, lone wolf) and (2) makes available unclassified versions of significant legal pleadings and opinions of the FISA court.