



To: Interested Persons

From: Timothy H. Edgar
National Security Policy Counsel¹

Date: June 7, 2005

Re: Section by Section analysis of S. 737, the Security and Freedom
Enhancement (SAFE) Act of 2005

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

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHIAR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

The bipartisan Security and Freedom Enhancement (SAFE) Act has been introduced in the 109th Congress by a diverse group of members led by a Western conservative – Senator Larry Craig (R-ID). Other supporters include John Sununu (R-NH), Lisa Murkowski (R-AK), Dick Durbin (D-IL), Ken Salazar (D-CO), and Russ Feingold (D-WI).

The SAFE Act provides common sense safeguards for a number of intrusive Patriot Act powers that share certain common themes. As a result of gag orders, or delayed notification, these powers 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 a judge in checking government abuse has been made less meaningful.

The SAFE Act would not repeal any provision of the Patriot Act, nor would it take away any government surveillance or law enforcement power conferred by the Patriot Act. Rather, it would help to add some judicial, Congressional and public oversight to Patriot Act powers. It is supported by an array of organizations on the left, right and center, including the American Civil Liberties Union, the American Conservative Union, Gun Owners of America and the Leadership Conference on Civil Rights.

Background: Intelligence and Criminal Investigations

The Patriot Act adds to the government's surveillance powers in both criminal and foreign intelligence investigations, and makes it easier for investigators to share information between these two types of investigations.

The Justice Department maintains that "[m]any of the tools the Act provides to law enforcement to fight terrorism have been used for decades to fight organized

¹ For further information, please contact Tim Edgar, Legislative Counsel (202) 675-2318 or Lisa Graves, Senior Counsel on Legislative Strategies (202) 675-2321.

crime and drug dealers.” This argument is based on a false equation of foreign intelligence investigations with terrorism investigations, and criminal investigations with non-terrorism investigations (i.e., “organized crime and drug dealers”).

The argument is simply wrong on both counts. Terrorists can be investigated with criminal powers, and foreign intelligence powers are not limited to terrorists.

- Criminal investigations are investigations of federal crimes, using powers like criminal search warrants and grand jury subpoenas. Criminal investigations are *not* limited to “ordinary” street crime or the Mafia, but can and do include investigations of terrorists, including Al Qaeda. Criminal investigations are also *not* limited to crimes that have already happened, but can also include the investigation *and prevention* of what are called “inchoate” crimes, including conspiracy, attempt, and solicitation. The guidelines for conducting criminal investigations (including what level of suspicion is required for certain intrusive techniques) are public.
- Foreign intelligence investigations are *domestic* investigations to obtain “foreign intelligence information,”² often using the special powers of the Foreign Intelligence Surveillance Act (FISA). 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 of American citizens and residents. The guidelines for conducting foreign intelligence investigations (including what level of suspicion is required for certain intrusive techniques) are classified.

Section-by-Section Analysis of S. 737

Section 1: Short Title

The short title of the bill – the Security and Freedom Enhancement Act of 2005 – reflects the belief of the sponsors that fundamental freedoms and civil liberties need not be at odds with taking appropriate measures to enhance national security.

Section 2: Reform of FISA roving wiretaps to include sensible privacy safeguards

Normally, a wiretap order must specify the telephone (or “facility”) to be monitored – just like a search warrant must specify home or location to be searched. Multipoint or “roving” wiretaps need only specify the target, *not* the

² “Foreign intelligence” and “foreign counterintelligence” are defined very broadly to include 1) information about the capabilities, activities or intentions of foreign governments, organizations, or persons, or 2) information the government thinks is useful to prevent a foreign attack, terrorism, or clandestine intelligence activities. 50 U.S.C. § 401a(1)-(3).

phone or facility, if a judge agrees the target is taking steps to thwart government surveillance by frequently changing phones.

Before the Patriot Act, roving wiretaps were available in criminal investigations (including terrorism investigations), subject to sensible privacy safeguards. Section 206 of the Patriot Act created “roving wiretaps” in foreign intelligence investigations, i.e., investigations using the special powers of the Foreign Intelligence Surveillance Act (FISA), but did not include these safeguards. The SAFE Act would add privacy safeguards to FISA roving wiretaps that are modeled on the existing safeguards in criminal investigations.

Because roving wiretaps are much more intrusive than traditional wiretaps, which apply to a single telephone or other device, when Congress considered whether to enact 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.

However, FISA roving wiretaps, as enacted by section 206 of the Patriot Act, do not include the common sense “ascertainment” safeguard. FISA roving wiretap authority was made even worse by the Intelligence Act for FY 2002, which authorized wiretaps where neither the target nor the device was allowed. As a result, FISA now allows “John Doe” roving wiretaps – wiretaps that can follow an unknown suspect from telephone to telephone based only on a potentially vague physical description, opening the door to widespread surveillance of anyone who fits that description, or anyone else who might be using that telephone.

The new roving wiretaps are especially troubling because they are FISA wiretaps. Ordinary criminal wiretaps – also called “Title III wiretaps” because they were first authorized by Title III of the 1968 Omnibus Crime Control and Safe Streets Act – require a judicial order based on probable cause that the communications to be intercepted will reveal activity relevant to one of a list of federal crimes called wiretap predicates. FISA wiretaps require no such finding. Instead, wiretaps may be authorized in secret based on the finding of the FISA court that there is probable cause the target of surveillance is a “foreign power” or an “agent of a foreign power” – that is, is acting for a foreign government or organization (including, but not limited to, a foreign terrorist organization).³

³ The “agent of a foreign power” standard has been undermined by section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, which allows foreign intelligence surveillance of so-called “lone wolf” terrorist suspects, i.e., non-U.S. persons who are involved in international terrorism, but who are acting alone. Section 6001 will also expire at the end of 2005, unless renewed by Congress. S. 737 does not address the “lone wolf” issue.

FISA roving wiretaps also 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 wiretap in 2004, with twelve criminal roving wiretaps in the entire 2002-2004 period.⁴

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.⁵ While the wording of the ascertainment requirement for wiretaps is different than the same requirement for oral interception,⁶ 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.

The language for oral interception is clearer and more straightforward. It provides simply that the interception "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." The SAFE Act simply chose the clearer of the two ascertainment standards provided in the criminal law.

The Justice Department also argues that FISA roving wiretaps are constitutional because they do require a physical description and, although they do not require probable cause of crime, they do require so-called "foreign agent" probable cause. The argument fundamentally ignores the need for specificity in government surveillance orders, a requirement that exists in addition to the requirement of "probable cause."

"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

⁴ Wiretap reports are available at the website of the Administrative Office of the U.S. Courts, at <http://www.uscourts.gov/library/wiretap.html>

⁵ Department of Justice, *USA PATRIOT Act: Sunsets Report* (April 2005), at 20.

⁶ See 18 U.S.C. § 2518(12) (ascertainment requirement for oral interception).

orders. In the landmark case *United States v. Donovan*, 429 U.S. 413 (1977), a majority upheld the federal 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.”⁷

The SAFE Act tightens the FISA roving wiretap so that it has the safeguards Congress believed were needed for roving surveillance in the criminal context. 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 3: Reform of “Sneak and Peek” criminal warrants.

Because of section 213 of the Patriot Act, notice of criminal search warrants can now be delayed for an indefinite “reasonable time,” if the judge finds an “adverse result” could occur if notice is given. “Adverse result” includes certain specific harms but also includes a “catch-all” standard of “otherwise seriously jeopardizing an investigation or unduly delaying a trial.” The power to delay notice of a search indefinitely based on a “catch-all” standard poses the danger of transforming ordinary criminal searches into intelligence “black bag jobs.”

Proponents of “sneak and peek” search warrants seldom acknowledge that, prior to passage of section 213 of the Patriot Act, there was *no statutory authority* for these warrants. The Federal Rules of Criminal Procedure – which governs the procedure for issuing search warrants – provided no express exception to the rule requiring service of warrants at the time a search was conducted.

While some courts had approved the practice in limited circumstances, two federal circuit courts of appeals that ruled on sneak and peek warrants prior to 9/11 had done so only pursuant to limitations that were swept away by the Patriot Act. For example, these courts had imposed a presumptive seven-day time limit for the delay.⁸ The Supreme Court had yet to decide whether general sneak and peek warrants were authorized by statute or the Constitution.

The Justice Department has relied on *Dalia v. United States*, 441 U.S. 238 (1979), claiming it not only approved “sneak and peek” warrants but dismissed a constitutional challenge to the practice as “frivolous.” In fact, *Dalia* approved a court order with delayed notice for the very specific purpose of installing bugging equipment for Title III surveillance – where notice would frustrate the entire purpose of the surveillance scheme Congress had approved. The Supreme Court has *never* addressed whether federal agents may delay notice of general search for evidence.

⁷ *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).

⁸ See *U.S. v. Villegas*, 899 F.2d 1324, 1337 (2nd Cir. 1990) (imposing a renewable seven-day notice requirement for “sneak and peek” searches); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (same).

In its most recent pronouncement on the subject, the Supreme Court, in an opinion written by Justice Thomas, cast doubt that such searches would be routinely approved. The Court held that the principle requiring notice for the execution of a warrant (often called the “knock and announce” rule) is not merely a common law principle, but is a constitutional rule based on the Fourth Amendment. *Wilson v. Arkansas*, 514 U.S. 927 (1995).

The SAFE Act restores the safeguard required by some federal courts that was overturned by section 213: that notice of federal criminal search warrants usually should not be delayed for longer than seven days. Delay can be renewed, based on an additional showing to the judge, for an unlimited number of additional periods of 21 days each.

In addition to imposing a time limit, the SAFE Act limits the reasons for “sneak and peek” warrants to four specific circumstances – that notice would cause (1) the life or physical safety of a person to be put in danger, (2) flight from prosecution, (3) destruction of evidence, or (4) intimidation of a witness. The Justice Department mischaracterizes the proposals to limit “sneak and peek” searches in saying they would allow a suspect’s “associates to go into hiding, flee, change their plans, or even accelerate their plots.” Clearly, the SAFE Act standard would permit a delay if the government could show any of these things.

The Justice Department continues to exclusively on cases of ordinary crime and drugs for examples of why sneak and peek searches are needed, rather than terrorism cases. The Justice Department also fails to acknowledge that the government can obtain an intelligence search warrant under FISA – which is always secret – for a physical search involving a suspected international terrorist, even where the SAFE Act’s standards for criminal “sneak and peek” searches could not be met.

As a result, it is clear that “sneak and peek” searches are *primarily* an investigative power for common crimes (not terrorism), and it is not surprising that the examples the government has used in its arguments to preserve this authority involve common crimes.

Sneak and peek warrants are becoming increasingly common. Between October 2001 and April 2003, the Justice Department reported it had obtained 47 “sneak and peek” warrants. Between April 2003 through January 2005 (a comparable, albeit slightly longer time frame), the Department obtained 108 warrants – or more than double the number.

In addition, at a hearing of the House Judiciary Committee on April 7, 2005, Attorney General Gonzales revealed some sneak and peek warrants had been issued with very lengthy delays (one as long as half a year). Six “sneak and peek” warrants had been issued with an *indefinite* delay – just as critics of the Patriot Act had feared. These lengthy and indefinite delays show the need for much stricter judicial oversight that would result from appropriate time limits.

Furthermore, the breadth of these “sneak and peek” warrants is clearly a problem. At a hearing before the Senate Judiciary Committee on April 6, 2005, Chairman Arlen Specter (R-PA) revealed that the majority of “sneak and peek” warrants are approved based on the “catch-all” language of jeopardizing an investigation or delaying a trial, rather than under more specific criteria that offer more meaningful judicial oversight. The argument for section 213 based on nationwide standards is also undercut by the government’s reliance on the “catch-all” provision, which is not a meaningful standard at all.

Section 4: Reform of FISA orders for private records, including library records, medical records, genetic information, and other “tangible things”

Perhaps no section of the Patriot Act has become more controversial than section 215, which allows 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 secretly gathering 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).

Indeed, Deputy Attorney General candidly acknowledged in testimony before the House Permanent Select Committee on Intelligence on May 11, 2005, that the only occasion on which the Justice Department would likely use a FISA order for records, instead of a criminal subpoena, is when the government has no “criminal hook” for its demand for private information – in other words, when the information is not relevant to any crime.

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 a government agent might decide is needed for intelligence reasons.

Section 215 of the Patriot Act swept away this limit. Section 215 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 a secret order from the FISA court. The order is no longer based on any suspicion the records relate to a foreign power, but is based merely on a certification by the government that the records are “sought for” a national security investigation. The judge is required to issue the order. The order contains an automatic and permanent gag order.

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. 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.

Section 215 is the subject of a court challenge 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 similar grounds. The district court has not yet decided in the Michigan case.

FISA records demands 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.

While 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 expanded scope and broader use of FISA records demands other constitutional problems with the statute under both the First Amendment and the Fourth Amendment. FISA records demands contain no explicit right to file a motion to quash the demand before a court on the ground that the demand is unreasonable or seeks privileged information. FISA records demands also bar the recipient from disclosing that the demand has been issued. This permanent secrecy order is imposed automatically, in every case, without any review by the judge, without any right to challenge.

Section 4 of the SAFE Act 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. In addition, it 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 SAFE Act also sets standards for a judicially-imposed, temporary secrecy order that can be challenged by the recipient of a records demand. Providing such a standard would not “tip off” the subjects of investigations where the government could convince a court of the need for secrecy. Rather, it would allow a court to hear, on a case-by-case basis, whether those or other arguments for such a secrecy order are supported by specific facts and really justify the prior restraint on speech the secrecy order imposes.

The SAFE Act also makes clear what the government has now conceded should be the law – that the secrecy order does not prevent recipients from discussing records demands internally or obtaining legal advice. Without public scrutiny, the potential for unreasonable “fishing expeditions” using a secret, unreviewable records power is simply too great.

Section 5: Reform of “National Security Letters” Power to Obtain Certain Records Without Any Court Review

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. Unlike records orders from the FISA court under section 215, these “national security letters” do not apply to all records or “tangible things.” Rather they can be used to obtain (1) a wide array of records from so-called “financial institutions” (a broadly-defined term that even includes pawnshops, car dealerships, casinos, and post offices), (2) credit reports, and (3) telephone, Internet and other communications billing or transactional records. 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.

Also unlike orders under section 215, national security 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. National security letters suffer from many of the same flaws as orders under section 215. They do not offer the recipient any right to challenge the order. They contain an automatic and permanent secrecy provision that bars the records holder from revealing the demand to anyone, again with no right to challenge. As a result of section 505 of the Patriot Act, they no longer require any statement that the records sought pertain to a foreign power or agent of a foreign power.

In *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a federal district court ruled against a “national security letter” records power expanded by the Patriot Act. Judge Marrero agreed 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.⁹

The district court ruling in *Doe v. Ashcroft* makes clear all these problems are severe enough to invalidate the entire national security letter statute – not just the portions amended by the Patriot Act. The SAFE Act would allow Congress to meet the objections of the court while preserving the existence of the national security letter power.

Section 6: Reform of Authority to Monitor Internet and Other Communications Without Probable Cause Using “Pen Registers” and “Trap and Trace” Devices

The Patriot Act expanded the use – without probable cause – of an intrusive surveillance technique that allows authorities to monitor a great deal of information generated by Internet and other communications traffic. Section 6 of the SAFE Act would ensure such techniques are at least limited to situations in which the government articulates specific facts showing the information would be relevant to the criminal or foreign intelligence investigation.¹⁰

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.

⁹ 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.

¹⁰ This standard is problematic for FISA pen/trap orders in that the government defines the scope of a foreign intelligence investigation; for FISA investigations, the pen/trap order need not be relevant to a criminal offense. A far more preferable standard would be the standard the SAFE Act uses for records searches – “specific and articulable facts” that the information “pertains to a foreign power or agent of a foreign power.”

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.

The problem for privacy is 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>.

The Patriot Act contains two sections that broaden the use of Internet surveillance, without probable cause, by extending the pen/trap surveillance technique from the telephone world to the Internet world. Section 214 broadens pen/trap authority under FISA. Section 216 broadens pen/trap authority for criminal investigations.

Both sections suffer from the same 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. The SAFE Act takes a first step toward remedying this problem by requiring orders for pen registers and trap and trace devices be based on “specific and articulable facts” that the information would be relevant to the investigation.

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.

Section 7: Reform of “Domestic Terrorism” Definition to Ensure Against Overbroad Application to Protest Organizations

Section 802 of the Patriot Act created an overbroad definition of “domestic terrorism” that could be used as a pretext for using investigative and other

powers against organizations that use civil disobedience tactics. Section 7 of the SAFE Act would address this problem by ensuring that “domestic terrorism” is defined by reference to a list of mostly serious federal crimes of terrorism.

Under the Patriot Act definition, any actions occurring primarily within the United States are “domestic terrorism” if they (1) “involve” a violation of state or federal criminal law, (2) “appear to be intended” to influence government policy or a civilian population by “intimidation or coercion” and (3) “involve acts dangerous to human life.” 18 U.S.C. § 2331(5).

This definition of “terrorism” is so broad that many legitimately fear it could cover the civil disobedience activities of diverse protest organizations, including Operation Rescue, Greenpeace, and the anti-globalization movement. Blocking entrances to abortion clinics, for example, could “involve” violations federal or state law and may certainly “appear to be intended” to influence government policy or a civilian population by “intimidation or coercion.” Blocking clinics under some circumstances involves “acts dangerous to human life” in that such actions could threaten the lives of the protesters (if protesters block traffic, for example) or interfere with the ability of women to get needed medical treatment. The anti-globalization movement is also known for civil disobedience tactics, such as chaining protestors together to block traffic, that could meet the definition

Section 802 does not create a separate crime of domestic terrorism. However, it does expand the type of conduct that the government can investigate when it is investigating “domestic terrorism.” This, in turn, triggers broad powers under other sections of the Patriot Act and other laws that have since been enacted.

Section 806 of the Patriot Act allows the civil seizure of assets without a prior hearing, and without a criminal conviction, of any persons engaged in “planning” any act of “domestic terrorism,” as well as any assets “affording a person a source of influence” over such an organization, as well as any assets derived from, or supporting, or involved in actions defined as “domestic terrorism.”

The breadth of the definition could easily lead to abuse, given the powers that are triggered. For example, an administration hostile to the anti-abortion movement could not only seize all assets of a direct action protest organization, it could also seize assets of its major donors (who therefore have “influence” over the organization) or the property (such as a church building) used for planning the protests or to facilitate that protests (such as a church bus). This could all occurred without prior notice or a hearing, and without any criminal conviction.

Other powers include:

- Disclosure of educational records – Sec. 507, allowing the government to get a court order for private educational records if the Attorney General

or his designee certifies that the records are necessary for investigating domestic or international terrorism.

- Disclosure of information from National Education Statistics Act – Sec. 508: allowing the government to get a court order for educational records that have been collected pursuant to the National Education Statistics Act, including information about academic performance to health information, family income, and race.
- Single-Jurisdiction Search Warrants – (Sec. 219), allowing the government to obtain a search warrant in any judicial district in which activities relating to the terrorism may have occurred, to obtain a warrant to search property or a person within or outside the district.
- Taxpayer Information – 26 U.S.C.A. Sec. 6103(i)(3)(C) has now been amended to require the Secretary of the Internal Revenue Service to provide taxpayer information to the appropriate Federal law enforcement agency responsible for investigating or responding to the terrorist incident.
- Regulation of biological agents and toxins – 42 U.S.C.A. Sec. 262a and 7 U.S.C.A. Sec. 8401 prohibits a person who is involved with an organization that engages in “domestic terrorism,” from gaining access to these regulated agents.

Because of these highly intrusive powers should only be triggered by serious criminal conduct, not crimes like trespass, blocking traffic or failure to obtain a permit for a march, the SAFE Act reforms the definition of “domestic terrorism.” Under the SAFE Act, the definition only applies to actions that constitute a crime on the list of federal crimes of terrorism under 18 U.S.C. § 2332b(g)(5). This was the original definition of “domestic terrorism” approved unanimously by the House Judiciary Committee in its consideration of the Patriot Act. The list is lengthy and includes well over forty crimes, ranging from bombing and hijacking to arson and computer crimes.

The SAFE Act would also change the definition to require that the actions must actually be intended to influence government conduct by intimidation or coercion, rather than that the actions “appear to be intended” to have that effect. Both these changes would go a long way towards reassuring the public that the “domestic terrorism” definition will be used to investigate genuine terrorists, not protest groups.

Section 8: Greater Public Reporting on FISA Surveillance

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, the criminal wiretapping law.

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. For example, the public report on Title III surveillance, while it omits sensitive law enforcement information, contains extensive aggregate and statistical information. The most recent public report on Title III surveillance was 247 pages long. By contrast, the Justice Department is required to report only the number of FISA applications and the number of orders granted (which is almost invariably the same number). The annual FISA “report” is merely a one or two-page letter.

The SAFE Act would begin to address this dramatic disparity by making public some additional information about FISA surveillance, building on section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004. The SAFE Act would make public the report to Congress required by that section.

That report includes

- disclosure of the total number of type of surveillance power – namely 1) wiretaps, 2) physical searches, 3) pen registers and trap and trace devices, and 4) “business” records searches.
- disclosure of the number of “lone wolf” surveillance orders – orders issued of suspects not connected to any foreign government or organization
- unclassified versions of significant legal pleadings and opinions of the FISA court.

Sensitive, classified FISA reports providing far more detailed information, currently provided to the House and Senate intelligence committees, would remain secret.

Some of this information – including the number of records orders – has been selectively made public by the Justice Department in its efforts to renew the Patriot Act. There has been no discernable impact on national security. Likewise, the Justice Department has disclosed the number of “roving wiretaps” under FISA, again with no discernable impact on national security. Finally, the Justice Department disclosed two major FISA court decisions, with redactions for classified information, interpreting provisions of the Patriot Act, again with no discernable impact on national security. Far more detailed information about criminal surveillance is revealed every year, with no discernable adverse impact on law enforcement.

The government simply cannot reasonably maintain that everything other than the total number of FISA orders issued each year must remain forever secret.

Conclusion: Restoring Checks and Balances

The Patriot Act provisions targeted for reform by the SAFE Act 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.

The controversy over the Patriot Act reflects the concerns of millions of Americans. Patriot Act resolutions have been passed in 379 communities in 43 states, including six state-wide resolutions. The resolutions have passed in strongly conservative states, such as Idaho and Alaska, as well as progressive states like Vermont. A nationwide coalition 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.

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. Passing the SAFE Act would give Congress a chance to begin the work of bringing the Patriot Act in line with the Constitution.

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

	<i>Surveillance power</i>	<i>Before Patriot Act</i>	<i>Now</i>	<i>Sur-sets?</i>	<i>SAFE Act safeguard</i>
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 FV2004 § 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.