



**Congressional Affairs Office  
Congressional Contacts**

Date Entered: 04/29/2003     Briefing     Hearing     Other    9/28/01

2003-740	Entered By: [redacted] 33
Subject:	Pen Register/Trap and Trace Administration Bill
CAO Contact Person:	[redacted]
DOJ Notification:	DOJ Date/Time: [redacted]
FBI Participants:	[redacted] Marcus Thomas FBI Lab
Other Participants:	[redacted] DOJ
Committees /Subcommittees:	House Judiciary
Members/Staff:	[redacted] Rep. From Cong. Goodlatte's office

b6  
b7c

**Details of Briefing:**

Staff asked for an explanation of the current practice when executing pen/trap orders then a brief description of what our proosed legislation would change several scenarios were discussed including both legal and technical discussions. System safeguards (ie audit logs/) were discussed. Discussion of some specific proposed legislative changes. Some staff expressed desire to legislate a defination of content to increase comfort level w/DCS 1000. [redacted]

[redacted]

b5

**Follow Up Action:**

[redacted]



**Congressional Affairs Office  
Congressional Contacts**

Date Entered: 04/29/2003

Briefing

Hearing

Other

CA/28/01

2003-738	Entered By:	33
Subject:	Pen Register/Trip and Trace - Administration Bill	
CAO Contact Person:	[Redacted]	
DOJ Notification:	DOJ Date/Time: [Redacted]	
FBI Participants:	[Redacted] Marcus Thomas-FBI Lab	
Other Participants:	[Redacted] DOJ	
Committees /Subcommittees:	House Leader Arney	
Members/Staff:	[Redacted] Leader Arney's office	

b6  
b7c

**Details of Briefing:**

Briefing was requested to clarify 101 of administration bill seeking nationwide pen/trap orders and clarification re applicability to internet communications. Arney not concerned about parity. The concern comes from the ability of FBI device (DCS 1000) to collect more than traditional pen/trap clarified legal issues and described checks and balances inherent in process currently in place i.e.: bifurcation of process, audit and logging capabilities. Suggestion that in situations where DCS 1000 is used and no prosecution results, the data obtained from device would be submitted to the authorizing CT for review.

**Follow Up Action:**

provide summary describing existing checks and balances.

~~SECRET//X1~~

SUBCOMMITTEE ON TERRORISM  
AND HOMELAND SECURITY HEARING QUESTIONS

*1. In the FY 2002 FBI Congressional Budget Justification for the National Foreign Intelligence Program (NIFP), which was written prior to the events of 9-11, the FBI highlighted in its Mission-based Analysis that "the FBI's NFIP focused its efforts on the 'Counterterrorism' mission". Two of its strategic goals were:*

- to build and maintain a dedicated cadre of experienced International Terrorism Agents; and*
- to forecast and identify the activities sponsored by foreign governments and terrorist organizations that pose a national security threat to the U.S.*

*The above stated, what steps were taken by the FBI prior to and after 9-11 to accomplish these strategic goals?*

(U) A basic understanding of the FBI Counterterrorism Division (CTD) Strategic Plan is necessary in order to understand the progress the FBI has made towards the two questioned strategic goals stated in the FY 2002 CBJB. The CTD consistently works to build and maintain experienced personnel and to forecast and identify threats to national security.

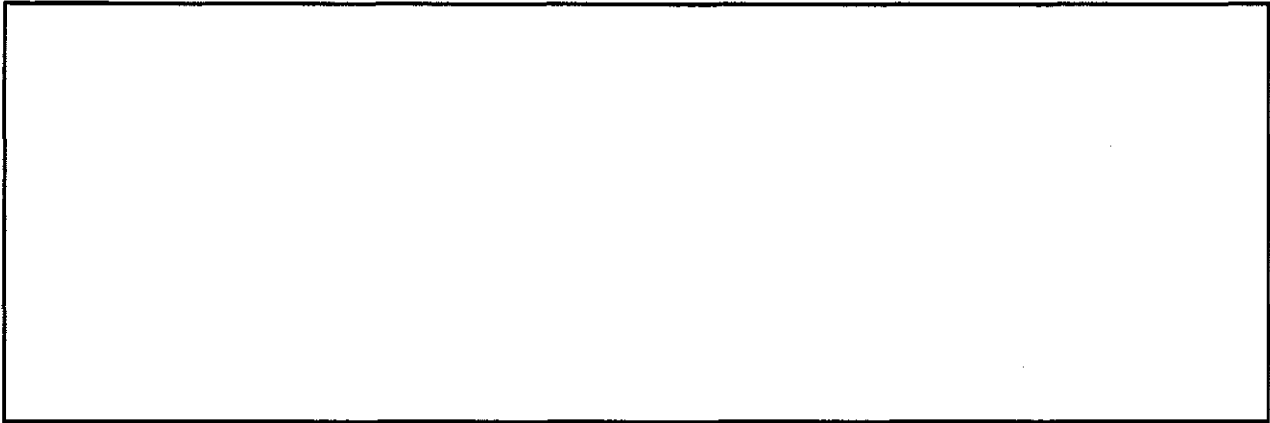
(U) Through comprehensive strategic planning initiatives at the Bureau and the Division level, the CTD has determined that building maximum feasible capacity throughout the CT program is the best method for addressing prevention. Building capacity consists of defining capacity, assessing capacity, identifying gaps, and addressing those gaps. Each goal is subjected to this process to ensure that it ultimately contributes to the CT mission of the FBI, which is to prevent, disrupt, and defeat terrorist acts before they occur.

**Background:**

(U) The three-tiered system of prioritizing programs in the FBI Strategic Plan is designed to focus expertise and resources on the most serious problems facing the nation. Tier One Programs include terrorism and foreign intelligence, both of which directly threaten the national or economic security of the U.S. Issues in these areas are of such importance to U.S. national interests that they must receive priority attention and, accordingly, the FBI's CT Program is a Tier One program, and constitutes the highest investigative program priority. The Strategic Plan requires Tier One initiatives to "develop and implement a proactive, and nationally directed program(s)."

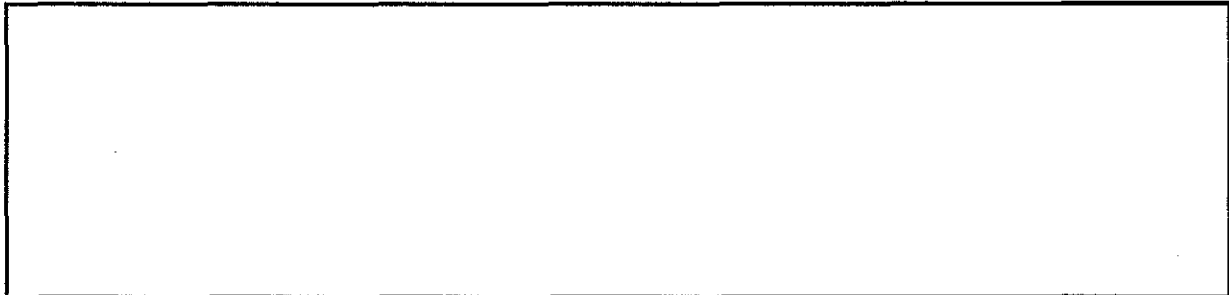
(U) In March 2000, the Assistant Director, CTD, initiated an effort to develop a comprehensive, dynamic strategic plan that addresses the critical needs of the CT programs. The first steps to developing a comprehensive program management strategy was to develop program goals and mechanisms for evaluating progress towards those goals. The goal of the CT Program, to identify, prevent, and deter acts of terrorism, is well-defined and well-understood.

~~SECRET//X1~~

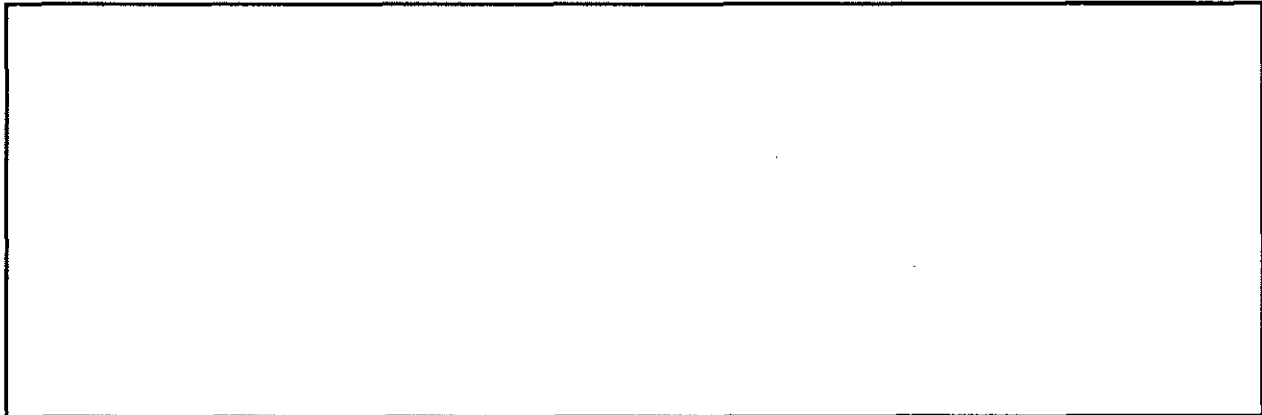


b5

*23. What, if any additional authorities, beyond those in the Patriot Act, would you like to have?*



b5



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

## A BILL

An Act to amend titles 18 and 47, United States Code, to permit prospective cell location orders.

Be it enacted by the House of Representatives and the Senate of the United States in Congress assembled,

### **SECTION 1. AMENDMENT TO 18 U.S.C. SEC. 2703 TO PERMIT RECORDS TO BE DISCLOSED PROSPECTIVELY.**

Section 2703 of title 18 United States Code is amended by adding the following paragraph at the end:

“(h) A court order under subsection (d) or a warrant under subsection (c)(1)(A) may require that records or other information (not including the contents of communications) be disclosed to a governmental entity prospectively.

(1) Standard. — The court shall issue an order or warrant requiring prospective disclosure if—

(A) in the case of a court order under subsection (d), the court finds that the application contains specific and articulable facts showing that there are reasonable grounds to believe that the prospective records or other information (not including the contents of communications) will be relevant and material to an ongoing criminal investigation; or,

(B) in the case of a warrant under subsection (c)(1)(A), the court finds that probable cause supports issuing a prospective warrant.

(2) Duration. — An order or warrant made prospective by this subsection may require prospective disclosure for a period not to exceed sixty days. Extensions of such an order or warrant may be granted, but only upon an application for an extension under this subsection and upon the judicial finding required by subsection (h)(1) of this section. The period of extension shall be for a period not to exceed sixty days.

(3) Nondisclosure. — An order or warrant made prospective by this subsection shall direct that—

(A) the order or warrant be sealed until otherwise ordered by the court; and,

(B) the person or entity who is obligated by the order or warrant to disclose records or other information prospectively to the applicant shall have the same nondisclosure obligations that section 3123(d) of this title imposes on a

person owning or leasing the line or other facility to which a pen register or a trap and trace device is attached.

(4) Scope and assistance. —

(A) An order or warrant made prospective by this subsection, upon service of that order or warrant, shall apply to any person or entity providing wire or electronic communication service or remote computing service in the United States whose assistance may facilitate the execution of the order or warrant. Whenever such an order or warrant is served on any person or entity not specifically named in the order or warrant, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order or warrant shall provide written or electronic certification that the order or warrant applies to the person or entity being served.

(B) Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of an order or warrant made prospective by this subsection, a provider of a wire or electronic communication service or a provider of remote computing services shall furnish such investigative or law enforcement officer all information, facilities and technical assistance including execution of such warrant or order unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the warrant or order pertains, if such installation and assistance is directed by a court. Unless otherwise ordered by the court, records or other information disclosed under such warrant or order shall be furnished to the officer of a law enforcement agency designated in the court order, at reasonable intervals during regular business hours for the duration of the order. Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) Emergencies. — Notwithstanding any other provision of this section, any individual identified in section 3125(a) of this title who reasonably determines that—

(A) an emergency situation, as described in section 3125(a)(1) of this title, exists and requires that records or other information (not including the contents of communications) be disclosed to a governmental entity prospectively before an order or warrant requiring such disclosure can, with due diligence, be obtained; and,

(B) there are grounds upon which an order or warrant could be entered under this section to require such prospective disclosure;

may require that records or other information (not including the contents of communications) be disclosed prospectively if, within forty-eight hours after the disclosure begins to occur, an order or warrant requiring such disclosure is issued in accordance with this section. In the absence of an authorizing order or warrant, the requirement to disclose prospectively shall immediately terminate when the records or other information sought are disclosed, when the application for the order or warrant is denied, or when forty-eight hours have lapsed since the disclosure began to occur, whichever is earlier.”

## **SECTION 2. PEN REGISTER AND TRAP AND TRACE AMENDMENT**

Section 3121(a) of title 18, United States Code, is amended by inserting "2703(h) or section" after "under section".

## **SECTION 3. AMENDMENT TO MOBILE TRACKING DEVICES STATUTE**

Section 3117(a) of title 18, United States Code, is amended by adding "Nothing in this section shall be construed to require a warrant when the Constitution of the United States does not require a warrant." at the end.

## **SECTION 4. AMENDMENT TO COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT**

Section 1002(a)(2) of title 47 U.S.C. is amended by inserting "Such call-identifying information may include information that may disclose the physical location of the subscriber or user if it is acquired pursuant to a court order or warrant, under section 2703 of title 18, or other lawful authorization;" after "(except to the extent that the location may be determined from the telephone number).”.





To: Interested Persons

From:   
National Security Policy Counsel

b6  
b7c

Date: March 28, 2005

Re: Patriot Act sunsets – What Congress should do

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](http://WWW.ACLU.ORG)

LAURA W. MURPHY  
DIRECTOR

NATIONAL OFFICE  
125 BROAD STREET, 10<sup>TH</sup> FL.  
NEW YORK, NY 10004-2400  
T/212.549.2300

OFFICERS AND DIRECTORS  
NADINE STROSSEN  
PRESIDENT

ANTHONY D. ROMERO  
EXECUTIVE DIRECTOR

KENNETH B. CLARK  
CHIEF, NATIONAL  
ADVISORY COUNCIL

RICHARD WACKS  
TREASURER

The USA PATRIOT Act was passed by Congress in 2001 just six weeks after the terrorist attacks of September 11. Although the act passed both Houses 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 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 power, Congress 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 enhance security and (b) that there is adequate supervision of the executive’s use of the powers to ensure protection of civil liberties.”<sup>1</sup>
- Second, “[i]f the power is granted, there must be adequate guidelines and oversight to properly confine its use.”<sup>2</sup>
- Third, because the issues of national security and civil liberties posed by anti-terrorism powers that are not part of the Patriot Act sunset are at least as serious as any posed by those provisions that do sunset, Congress should undertake a broader review of anti-terrorism powers, both within and outside of the Patriot Act, using the same standard of review.

<sup>1</sup> Final Report of the National Commission on Terrorist Attacks Upon the United States (“The 9/11 Commission Report”) 294-95 (2004) (boldfaced recommendation)

<sup>2</sup> *Id.*

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

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. Congress may also decide that some powers outside of the Patriot Act's sunset provisions should be reviewed at a later time.

The lack of meaningful information about many powers is a direct result of the excessive secrecy of the Executive Branch. In any case where sufficient information is not available to undertake a thorough review, Congress should either allow the provisions to expire or set a new sunset date, with additional reporting requirements to facilitate a proper review, rather than cede those powers permanently to the Executive Branch.

*Patriot Act: Greater Secrecy, Less Meaningful Review*

In reviewing those provisions of the Patriot Act that are set to expire at the end of the year, Congress should reserve its most searching review and examination for those provisions that pose the greatest challenges to civil liberties.

A number of these provisions 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 a judge in checking government abuse has been made less meaningful.

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. It is important to understand the difference between the two.

- 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 of the activities of foreign governments or organizations, including foreign terrorist organizations, 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. The guidelines for conducting foreign intelligence investigations (including what level of suspicion is required for certain intrusive techniques) are classified.

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, and vice versa. For example, traditional law enforcement warrants are properly executed openly as a general rule, even though intelligence searches have long been conducted in absolute secrecy. Conversely, grand juries have extraordinary powers to compel documents and testimony for investigative purposes that would be entirely inappropriate in the hands of intelligence agents. Criminal and foreign intelligence investigations are simply different, and pose very different dangers to civil liberties.

In the upcoming debate over the Patriot Act, Congress should pay particular attention to the following surveillance techniques:

#### Secret Searches of Homes and Offices

A government search of a home or office requires a warrant based on probable cause under the Fourth Amendment. As a general rule, the owner of the home or office is entitled to a copy of the warrant and notice of the search. Two sections of the Patriot Act erode this general rule.

- Section 218 lowers the standards for using secret “foreign intelligence” physical search powers (as well as wiretaps) in federal investigations. Section 218 is subject to the Patriot Act’s sunset clause.
- Section 213 makes criminal search warrants more like intelligence “black bag jobs” because it makes it easier for the government to delay notice of the execution of a search warrant. Section 213 is permanent.

Congress should examine both sections and act to restrain this trend of making searches of a home or office more and more secret.

*Section 218: foreign intelligence “black bag jobs.”* Foreign intelligence investigations include special powers to secretly search a home or office, without ever notifying the owner, where there is probable cause that the home or office contains information about the activities of an agent of a foreign power (but not necessarily any evidence of crime) and agents obtain a special warrant from the secret court established by FISA. One limit on this power, prior to the Patriot Act, was that government officials had to certify that the *primary*

*purpose* of the search was for “foreign intelligence.” 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.

When examining section 218, Congress should explore ways to tighten the use of “foreign intelligence” searches for other purposes, such as criminal investigations. Without re-building the much-maligned “wall” between foreign intelligence and criminal investigations, Congress should clarify that foreign intelligence investigations should not be directed by federal prosecutors, although prosecutors and criminal investigators should be allowed to be fully briefed on such investigations. Congress should also explore making available to the defense more information, using the carefully-crafted Classified Information Procedures Act (CIPA), than is currently allowed when the fruits of foreign intelligence investigations are used in criminal trials.

*Section 213: secret criminal search 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 indefinitely delay a search based on a “catch-all” standard poses the danger of transforming ordinary criminal searches into intelligence “black bag jobs.”

Congress should insist on taking another look at section 213, although that section does not sunset. Congress should restore 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. Congress should also eliminate the “catch-all” provision for obtaining a secret search warrant, allowing such warrants only when *specific* harms would otherwise result.

Congress can put responsible limits on secret criminal search warrants without doing away with the intrusive practice altogether. In the 108th Congress, bipartisan legislation amending the Patriot Act would have put such limits on secret criminal search warrants.<sup>3</sup> Similar legislation is expected to be introduced in the 109th Congress.

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

Congress has authorized federal judges to issue electronic surveillance orders in serious federal criminal cases and in foreign intelligence cases— including wiretaps of telephone conversations and intercepts of the content of other electronic communications (faxes, e-mail, etc.). Such wiretaps are subject to the Fourth Amendment’s demands for a judicial warrant, based on probable cause.

---

<sup>3</sup> Security and Freedom Ensured Act, S. 1709, at § 3.

“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 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.”<sup>4</sup>

The Patriot Act erodes this basic constitutional rule:

- Section 206 creates “roving wiretaps” in foreign intelligence cases. 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.
- Section 207 greatly increases the length of time that foreign intelligence wiretaps may be used without any judicial oversight – from 90 days to 6 months for the initial order, with renewals allowing surveillance to continue for a year before require judicial approval. Section 207 is subject to the Patriot Act’s sunset clause.

In examining these and other electronic surveillance provisions of the Patriot Act, Congress should pay special attention to dangers posed to civil liberties by expanding secret, foreign intelligence wiretap powers not subject to the normal criminal probable cause requirements of standard wiretaps.

Federal 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. Foreign intelligence wiretaps require no such finding. Instead, wiretaps may be authorized based on the finding of the secret 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).<sup>5</sup>

---

<sup>4</sup> *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).

<sup>5</sup> 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

*Section 206: Foreign intelligence "roving wiretaps."* "Roving wiretaps" are a particularly potent form of electronic surveillance, allowing the government to obtain a single wiretap order that follows a target as the target uses different telephones or devices to communicate. 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 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.

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 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.

Congress should tighten the FISA roving wiretap so that it has the same safeguards for privacy as criminal roving wiretaps. 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 207.* 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. Congress should shorten these periods to something more reasonable -- certainly no more than six months. 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

---

in international terrorism, but who are acting alone. Section 6001 will also expire at the end of 2005, unless renewed by Congress.

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

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>.

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 214 is subject to the sunset clause. Section 216 broadens pen/trap authority for criminal investigations. Section 216 is permanent.

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. To right this balance, Congress should:

- 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](http://www.aclu.org)) but not of webpages visited (like [www.aclu.org/patriotact](http://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.

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

Perhaps no section of the Patriot Act has 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 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).

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. The Patriot Act eliminated this basic limit for records searches, including the power under the Foreign Intelligence Surveillance Act to obtain 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 Foreign Intelligence Surveillance Court. 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.
- 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 is permanent.

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 – one in New York and one in Michigan. In the New York case, *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, 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. 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.

While 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 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 or only with the threat of such a letter.

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.

The expanded scope and broader use of both FISA records demands and national security letters has exacerbated other constitutional problems with the statute under both the First Amendment and the Fourth Amendment. Unlike almost every other type of subpoena or records demand, neither statute contains any 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. Similarly, both types of records demands 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 a judge, without any right to challenge. The district court ruling in *Doe v. Ashcroft* makes clear these problems are severe enough to invalidate the entire national security letter statute – not just the portions amended by the Patriot Act.

Congress should restore the requirement of “specific and articulable facts giving reason to believe” the records involve an “agent of a foreign power” for both FISA records demands and national security letters. In addition, Congress should take the opportunity to fix the additional problems of the FISA records law and national security letters. Congress should make explicit the right to file a motion to quash the records demands because they are unreasonable, contrary to law, or seek privileged information. Congress should also set standards for a judicially-imposed, temporary secrecy order that can be challenged by the recipient of a records demand. Congress should also make 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.

#### Providing Material Support for Lawful, Nonviolent Activities of a Group on the Terrorist Organization List

Knowing providing financial or other assistance in order to aid an individual or group in committing acts of political violence is rightly a serious federal crime. Unfortunately, the law defining terrorism and prohibiting material support of terrorism sweeps far more broadly, and can apply to acts of civil disobedience and support of genuine humanitarian activities. The Patriot Act exacerbated the problem of a definition of terrorism that sweeps far too broadly:

- Section 805 of the Patriot Act broadened the crime of providing material support to a designated foreign terrorist organization to include “expert advice and assistance.” A defendant need not intend to help the organization engage in violence. The forms of advice and assistance that are barred include purely nonviolent, humanitarian assistance. Perversely, as one federal court noted in a challenge to the law, it has even prevented a human rights organization from advising a rebel group on the State Department list of foreign terrorist organizations on its obligations under the law of war to avoid civilian casualties.<sup>6</sup>

---

<sup>6</sup> *Humanitarian Law Project v. United States Dep't of Justice*, 352 F.3d 382, 389 (9th Cir. 2003). After that case had been decided, the statute was amended by the Intelligence Reform and Terrorism Prevention Act of 2003 to include a requirement, which the Ninth Circuit had said was required by the Constitution, that a defendant have some knowledge of the organization's designation or unlawful activities to be prosecuted. As a result of Congress's action, the Ninth Circuit vacated its earlier ruling and remanded the case to the district court for further proceedings. See *Humanitarian Law Project v. United States Dep't of Justice*, 393 F.3d 902 (9th Cir. 2004).

- Section 802 of the Patriot Act defined “domestic terrorism” to include any actions that involve a violation of state or federal law, include “acts dangerous to human life” and are intended to influence government policy or a civilian population. The definition could cover the civil disobedience activities of many protest organizations, including the anti-abortion group Operation Rescue and some environmental activists. While “domestic terrorism” is not itself a separate crime, the definition triggers a host of enhanced surveillance and other powers, and the administration has proposed legislation to use the definition as a trigger for the death penalty.

Congress should reign in the definition of terrorism to ensure that it does not include civil disobedience or legitimate charitable or humanitarian activity.

*Section 805: Material Support.* Proponents of the material support law often argue that money provided for the legitimate, charitable activities of a group on the designated foreign terrorist list can be diverted to supporting violence. They argue it is necessary to prohibit sending money to an orphanage or soup kitchen controlled by an Islamist militant organization like Hamas because there is no way to ensure the money is not diverted to support suicide bombing attacks.

Whatever the merits of that argument with regard to financial assistance, it does not apply to “expert advice or assistance,” “training,” or other pure association. A doctor who works in a rebel organization’s medical clinic is not a combatant and is not assisting in violence. Likewise, a technician who provides support for a website engaged purely in lawful political speech, and not in incitement to imminent lawless action, is clearly engaged in constitutionally-protected association.

The list of designated foreign terrorist organizations includes a number of rebel organizations involved in regional conflicts around the globe. Fears of prosecution for material support of terrorism have complicated the work of Oxfam International, Doctors without Borders, and a number of other humanitarian organizations who must obtain the tacit cooperation of rebel groups to assist civilians in territory under rebel control. For example, in the recent Tsunami disaster, the Sri Lanka government, the Tamil Tigers (a designated foreign terrorist organization) and relief organizations cooperated to ensure the prompt delivery of humanitarian supplies.

The Intelligence Reform and Terrorism Prevention Act of 2004 takes a small step forward by requiring a defendant to know that material support is for an organization on the designated terrorist list or that the organization is involved in terrorism. Congress should also enact an intent requirement that makes assistance criminal only if the defendant intended to further the organization’s violent activities. Doctors without Borders should not have to fear prosecution if one of its volunteers provides medical aid to a Tamil Tiger fighter whose village was destroyed in the Tsunami.

At the very least, Congress should make such an intent requirement the law for prosecutions involving “expert advice and assistance,” “training,” or other non-monetary assistance of a purely humanitarian nature.

*Section 802: Definition of “Domestic Terrorism.”* Under the Patriot Act’s 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 they 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 or make it illegal provide “material support.” However, it does expand the type of conduct that the government can investigate when it is investigating “domestic terrorism,” which triggers broad powers under other sections of the Patriot Act and other laws that have since been enacted, including:

- Seizure of assets – Sec. 806, allowing the civil seizure of assets without a prior hearing, and without a criminal conviction, of persons involved in “domestic terrorism.”
- 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 the chilling effect of this definition on ideologically diverse protest groups, Congress should reform the definition of “domestic terrorism” so that it applies only to actions that constitute a serious federal crime, such as a crime on the list of federal crimes of terrorism under 18 U.S.C. § 2332b(g)(5).

#### Indefinite Detention Without Criminal Charge

Lengthy incarceration is the most serious deprivations of liberty the government can impose short of the death penalty. For that reason, the government bears the burden of proving a defendant guilty of a crime beyond a reasonable doubt following a trial that adheres to time-honored principles of due process, including the right to a lawyer and the right to confront the government’s evidence.

When Congress considered the administration proposal that became the Patriot Act, it focused more attention on the detention provisions than on any other single provision of the act. Congress balked at the administration’s original proposal for blanket authority to detain any non-citizen suspected of terrorism indefinitely, without criminal or immigration charges and without judicial review. Instead, when it crafted section 412 of the Patriot Act, Congress required criminal or immigration charges to be filed within seven days, preserved judicial review by habeas corpus, and, for lengthy detentions, required six-month reviews to determine if the detainee continued to pose a threat to national security. Only non-citizens were made subject to the special detention procedures of section 412 of the Patriot Act.

The administration never invoked section 412 of the Patriot Act. Instead, it used a variety of legal stratagems to detain both citizens and non-citizens indefinitely without criminal charge and, in some cases, without any meaningful access to counsel or ability to confront the accusations on which the detention was based. These included:

- *Domestic detention of so-called “enemy combatants.”* Invoking the President’s commander-in-chief authority and the Congress’s authorization of force after 9/11, the administration detained both citizens and non-citizens suspected of terrorism without charge, without access to a lawyer, and without the ability to confront the accusations against them. In addition to many hundreds of enemy combatants detained abroad and held at Guantanamo Bay, Cuba, the administration detained three individuals, including two American citizens, within the United States.

- *Widespread use of the “material witness” statute.* The Department of Justice arrested large numbers of suspects, including American citizens, as “witnesses” for a grand jury investigation, using a statute that had previously been used almost exclusively in rare cases where a crucial witness was expected to flee rather than appear at a trial. In many cases, suspects were never brought before a grand jury to testify and requests for videotape depositions or other arrangements to avoid detention were denied.
- *Immigration detentions on minor, pretextual charges.* Hundreds of Arab and Muslim men were detained shortly after 9/11, often for minor, pretextual immigration infractions that, in ordinary circumstances, could be resolved easily with an opportunity to file the right immigration forms. The men were labeled “special interest” detainees and denied release on bond or the right to leave the country rather than face continued detention. An internal Justice Department investigation criticized the manner in which detainees were labeled terrorism suspects and criticized impediments to their access to lawyers and other denials of their legal rights.<sup>7</sup>

Congress should use its review of the Patriot Act to examine these strategies for detaining persons without criminal charge and, in many cases, without meaningful access to attorneys and the ability to confront the evidence against them. While enemy combatant detentions, detentions on material witness warrants and pretextual immigration detentions do not directly involve Patriot Act powers, they are clearly relevant to a review because they appear to be designed to evade clear limits on detention that Congress included in section 412 of the Patriot Act.

Congress should reign in detentions without criminal charge, which have resulted in widespread abuses of the civil liberties of both American citizens and immigrants. The strong presumption of American law – that a suspect, including a terrorism suspect – is innocent until proven guilty lacks all force if the government can avoid the scrutiny of a criminal trial. At the very least, Congress should:

- *Refuse any explicit authorization of “enemy combatant” detentions.* The government’s arguments for a Commander-in-Chief power to detain suspects indefinitely without any legal process have not fared well in the courts. Congress should not “save the day” for this doomed legal theory by authorizing indefinite detention without charge for the first time since Japanese internment, even with enhanced procedural safeguards. The government bears a very heavy burden in establishing that, even with the

---

<sup>7</sup> Office of the Inspector General, U.S. Dep’t of Justice, *The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks* (June 2003). See also Office of the Inspector General, U.S. Dep’t of Justice, *Supplemental Report on September 11 Detainees’ Allegations of Abuse at the Metropolitan Detention Center in Brooklyn, NY* (December 2003). Both reports are available on the Inspector General’s website at <http://www.usdoj.gov/oig/igspeccr1.htm>

expanded anti-terrorism powers of the Patriot Act and other statutes, it cannot detain terrorism suspects on criminal or terrorism-related immigration charges.

- *Reign in abuse of the “material witness” law.* Congress should provide strict limits for the use of the material witness law, particularly in grand jury proceedings, which may last months or years. Congress should provide a strong presumption in favor of videotaped depositions or other techniques to allow the government to obtain witness testimony without resorting to detention.
- *Ensure meaningful control of immigration detentions.* Congress should reverse regulations, adopted after 9/11, that weakened the power of the Justice Department’s Executive Office of Immigration Review (EOIR). EOIR immigration judges and appeals panel members should not have their decisions to release detainees on bond automatically stayed simply at the request of an attorney for the government side.

*Conclusion: Restoring Checks and Balances*

Congressional 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. To date, resolutions in opposition to parts of the Patriot Act and other actions that infringe on fundamental rights have been passed in 372 communities in 43 states including four state-wide resolutions. These communities represent approximately 56.2 million people who are calling for reform of the Patriot Act.

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.



Date: 5-21-2009  
Classified by: 60322/LRP/PLJ/SDB  
Reason: 1.4 c,g  
Declassify On: 5-21-2034

~~SECRET~~



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

b6  
b7c

August 4, 2003

To: [redacted]  
[redacted] Counterterrorism Law Unit I

ALL INFORMATION CONTAINED  
HERE IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

From: [redacted]

Re: Draft Memorandum Regarding Email Header Information and the Definition of "Content"

### **I. Introduction**

This memorandum will address the question whether email "header" information is properly considered to be "content" in the context of Pen Register authority granted pursuant to the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. 1801, *et. seq.* (2001). The road to be traveled in search of the answer to this question is a winding one, with layovers in the courts and in the criminal code. [redacted]

b5

### **II. What is Header Information?**

While a complete answer to this question is beyond the scope of this memorandum and, quite frankly, outside the ken of the drafter, a wee bit of an understanding of "header" information is a necessary starting point for the discussion. As explained by Orin Kerr in his superb article entitled *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, every communications network distinguishes between "content" information and "envelope" information. Envelope information is the addressing and routing information used by the network to deliver the content, or substance, of the message.

In the context of a letter, the "envelope" information is the information derived from the outside of the envelope such as the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed. The content is the information contained in the letter itself, sealed safely inside.

Professor Kerr explains that those principles translate to the internet quite readily in the case of email. Addressing information, quite like the outside of a standard envelope placed into the mail, is contained in a "mail header." These mail headers, Professor Kerr explains, are "digital postmarks" that accompany every email and carry information about the delivery of the mail. *Id.* at 611. A full mail header may contain a dozen or more lines comprised of various characters

<sup>1</sup> 97 Northwestern University Law Review 607 (Winter, 2003).

~~SECRET~~

frequently displayed in a fashion that is indecipherable to a lay reader. Those characters, however, are deliberately and sequentially arranged to ensure the delivery of the content to its intended destination. When complete, the header information is a travelogue of the message as it traveled through various weigh stations on the network en route to its final destination. [REDACTED]

b5

[REDACTED]

[REDACTED]

b5

## II. Title III: The Lower Courts and New York Telephone

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2520, prohibits wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers who are engaged in the investigation of certain major crimes specified in the Act. At the time of its passage, however, Title III did not have pen register devices within its purview.

Simply stated, at the time of its passage, Title III was concerned only with court orders "authorizing or approving the interception of a wire or oral communication...." 18 U.S.C. 2518 (1). Congress defined "intercept" to mean "the *aural acquisition* of the *contents* of any wire or oral communications through the use of any electronic, mechanical or other device. 18 U.S.C. 2510 (4) (emphasis added). Congress did not intend by this definition to embrace pen registers and, indeed, expressed its intent that such devices were expressly excluded from the coverage of the act. *See* Senate Report No. 1097, 90th Cong., 2d Sess. 90 (1968)("[o]ther forms of surveillance are not within the proposed legislation...The proposed legislation is not designed to prevent the tracing of phone calls. The use of a 'pen register,' for example, would be permissible").

That intent, as further devined by courts later called upon to interpret the act, apparently stemmed from two sources within the definition of "intercept." First, it was understood that because pen registers do not hear sound, they were incapable of aurally acquiring the contents of a wire or oral communication. *See, e.g., United States v. Bell Telephone Co.*, 531 F.2d 809, 811 (7th Cir. 1976); *United States v. Clegg*, 509 F.2d 605, 610 (5th Cir. 1975); *United States v. Falcone*, 505 F.2d 478, 482 (3d Cir. 1974). Second, in the case of *United States v. New York Telephone Company*, 434 U.S. 159 (1977), the Supreme Court concluded as well that because pen registers "do not acquire the 'contents' of communications...they do not "intercept" communications as defined in the act.

More specifically, the Court in *New York Telephone* defined a pen register as

a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.

~~SECRET~~

*Id.* at 161, note 1.

The statutory definition of "contents" with which the *New York Telephone* Court was concerned was found at 18 U.S.C. 2510(8) and provided that the word contents, "when used with respect to any wire or oral communication" includes

any information concerning the identity of the parties to [the] communication or the existence, substance, purport, or meaning of [the] communication.

*United States v. New York Telephone*, *supra*, 434 U.S. at 167, note 11.

The Court concluded that even as defined, pen registers do not acquire content. In explaining its conclusion, the Court explained

These devices do not hear sound. They disclose only the telephone numbers that have been dialed--a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

*Id.* at 167.

Thus, in December of 1977, the Supreme Court concluded, as had several Circuit Courts of Appeal before it, that the restrictions of Title III did not apply to pen register devices. That conclusion was based, at least in part, on the conclusion that pen registers did not acquire the "contents" of wire communications as that term was defined in 18 U.S.C. 2510(8).

### **III. The Foreign Intelligence Surveillance Act of 1978**

In 1978, Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801-1862 (2002). The FISA statute authorizes a member of a specially denominated court to grant an application for an order approving electronic surveillance to "obtain foreign intelligence information" if there is probable cause to believe that the target of the electronic surveillance is a "foreign power" or "an agent of a foreign power." 50 U.S.C. 1805 (a)(3).

"Electronic surveillance" was defined, in part, as the "acquisition...of the contents of any wire or radio communication." *See* 50 U.S.C. 1801 (f)(1)-(3).<sup>2</sup> Like Title III, enacted ten years earlier, FISA did not, within the terms of the statute, expressly provide for pen registers as a distinct electronic surveillance-type device.

---

<sup>2</sup> Electronic surveillance was also defined as "the installation or use of an electronic, mechanical, or other surveillance device...for monitoring to acquire information, *other than from a wire or radio communication...*" 50 U.S.C. 1801 (f)(4).

~~SECRET~~

Similarly, Congress defined FISA "content" consistently with the definition then found in Title III.<sup>3</sup> Congress, however, was not enamored with the decision of the Supreme Court only seven months earlier in *New York Telephone*. Indeed, labeling the Court's conclusion that a pen register did not acquire the contents of a wire communication a "gratuitous" "suggestion", Congress expressly provided that "it is the intent of this committee that pen registers *do* acquire 'contents' of 'wire communications.'" House Report 95-1283 *accompanying* H.R. 7308, 95th Cong., 2d Sess. (June 8, 1978) (emphasis added).

The drafters further explained

[t]he term 'contents' specially mentions the identity of parties and 'identity' includes a person's phone number, which can as effectively identify him as the mention of his name. Moreover, the definition of 'contents' includes information concerning the 'existence' of a communication. When a person dials another person's telephone number, whether or not the other person answers the phone, this is a communication under this bill.

*Id.*

Importantly, Congress was acutely aware that this bill applied to the foreign intelligence milieu and not to the investigation of a limited class of domestic criminal offenses. The drafters noted, for example, that "signals to a spy may be conveyed merely by having his phone ring." *Id.* The fact "that the target of the pen registers has attempted to communicate with another person at a particular phone," said Congress, "is information concerning the 'existence' of the communication." *Id.* The rejection of *New York Telephone* was clear and unambiguous.

#### **IV. Smith v. Maryland**

Within a year of the passage of FISA, pen registers were back before the Supreme Court. Unlike *New York Telephone*, however, the case of *Smith v. Maryland*, 442 U.S. 735 (1979) presented to the Court a question of Constitutional, rather than statutory interpretation.

In *Smith*, the Court was squarely presented with the question whether the installation and use of a pen register device constitutes a search within the meaning of the Fourth Amendment. The facts were relatively straight forward. After a robbery victim had received threatening and obscene telephone calls from a man identifying himself as the robber, the telephone company, at the request of the local police, installed a pen register at the company's central offices to record the numbers dialed from the suspect's home telephone. The police had not obtained a search warrant or a court order to support their request of the telephone company. Based, among other

---

<sup>3</sup> To account for the type of electronic surveillance contemplated by 50 U.S.C. 1801(f)(4), Congress, in drafting the FISA content definition, deleted the modifying clause "wire or oral communication" from the first line of the definition. 50 U.S.C. 1801 (n). In all other respects, the FISA content definition is the same as the original Title III definition of content.

~~SECRET~~

things, that the pen register established that a call had been made from the suspect's telephone to the victim's telephone, the defendant was convicted. On appeal, the defendant claimed that information gleaned from the pen register was unconstitutionally obtained in violation of the fourth amendment. The Supreme Court disagreed.

The *Smith* court began its analysis by adopting the reasoning of *New York Telephone*, decided only eighteen months earlier. More specifically, the court, quoting liberally from *New York Telephone*, concluded that pen registers are devices of "limited capabilities" and as such, "do not acquire the contents of communications." *Id.* at 741-42.

The focus of the inquiry thus narrowed to the telephone numbers dialed by the defendant, the court went on to conclude that even if the defendant had a subjective expectation of privacy in the telephone number, such an expectation was not one that society was prepared to accept as reasonable. The Court explained that all telephone users realize that they must convey phone numbers to the telephone company, since it is through their switching equipment that their calls are routed to the intended recipient. All callers realize as well, reasoned the Court, that the telephone company necessarily records and maintains such information for billing purposes. Given these realities, said the Court, "it is too much to believe that telephone subscribers...harbor any general expectation that the numbers they dial will remain secret." *Id.* at 743. Because the defendant voluntarily turned over to a third party the telephone number he now argues should be suppressed, he surrendered any legitimate expectation of privacy. *Id.* at 743-44.

Thus, by June of 1979, the Supreme Court had concluded that, as defined, pen registers do not acquire "contents" as defined by Title III and that acquisition without a warrant of telephone numbers through the use of a pen register does not offend the fourth amendment. For its part, Congress had, with the passage of FISA, clearly expressed its disagreement with the statutory analysis of *New York Telephone*. Congress would not speak again on the issue of pen registers, however, for seven more years.

#### **V. The Electronic Communications Privacy Act of 1986**

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"). That act established, for the first time, a separate pen register provision in Title 18 of the United States Code. *See* 18 U.S.C. 3127 (3). In that section, a pen register was defined, in part, as a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line...".

Acknowledging the decisions of the Supreme Court in *New York Telephone and Smith v. Maryland*, Congress also amended the Title III definition of "contents." More specifically, the definition was amended to exclude from the definition the identity of the parties or the existence of the communication. In the legislative history that accompanied the ECPA, Congress explained the amendment by acknowledging that the Supreme Court had "clearly indicated that the use of pen registers does not violate either [Title III] or the fourth amendment." Senate Report to accompany Pub. L. 99-541 (October 17, 1986). This legislation, said the drafters, was to "make[] that policy clear."

Congress expressly provided, however, that this amendment "does not affect the installation or use of pen registers under the Foreign Intelligence Surveillance Act..." *Id.*

b5

~~SECRET~~

~~SECRET~~

however, unlike newly amended Title 18, the FISA statute still was without its own pen register provision. Thus, the acquisition of pen register type information in the FISA context was acquired only in conjunction with an order authorizing full electronic surveillance and interception of communications. It is unclear why Congress waited an additional twelve years before adding a pen register provision to the FISA statutory scheme.

#### **VI. Intelligence Authorization Act of 1999**

As part of the intelligence community appropriations bill for 1999, Congress authorized the government to seek the installation and use of a pen register or trap and trace device in connection with investigations seeking foreign intelligence information or information concerning international terrorism. *See* 50 U.S.C. 1841-42.

In providing for such authority, Congress acknowledged that, absent such a provision, the complete FISA predicate for actual interception of the oral or verbal contents of a communication must be satisfied before pen register-type information may be obtained by the government. Senate Report 105-185 *accompanying* Pub. L. 105-272 (May 7, 1998). The drafters went on to say

That predicate is designed to satisfy strict constitutional requirements for the conduct of a "search" within the meaning of the Fourth Amendment. However, and subsequent to passage of FISA in 1978, the Supreme Court held in *Smith v. Maryland* [citation omitted] that accessing numbers dialed to contact another communications facility is not a Fourth Amendment "search." Thus, current procedures impose a standard that is more rigorous than the constitution requires. [This] section establishes a predicate for the use of pen registers or trap and trace devices that is consistent with [that] opinion and is analogous to the statutory standard for the use of these devices in criminal investigations.

*Id.*

Thus, in 1999, Congress sought in FISA to emulate the criminal pen register provisions found in the ECPA and Title III. Further evidence of Congressional intent to import criminal pen register principles into FISA is found in the definitional section of the 1999 amendment. Congress did not write new definitions for either "pen register" and/or "trap and trace device." Rather, the newly amended FISA statute adopted the ECPA definitions for those two devices. *See* 50 U.S.C. 1841 (2), adopting 18 U.S.C. 3127 (3), (4). Moreover, the process for obtaining an order to install a pen register or trap and trace device under FISA is substantially similar to the process under the pen register section of the ECPA. *Compare* 50 U.S.C. 1842(b)(d) *with* 18 U.S.C. 3122-3123.

What Congress did not do, however, was adopt the Title III definition of "contents" as amended by the ECPA in 1986. Thus, despite almost overwhelming evidence of Congressional intent to incorporate into the FISA statutory scheme the pen register principles expressed by the Supreme Court in *New York Telephone* and *Smith v. Maryland*, and later codified in the 1986

~~SECRET~~

[Redacted]

b5

**VII. The Patriot Act Amendments of 2001<sup>4</sup>**

The Patriot Act Amendments of 2001 resulted in three significant changes to FISA pen register authority and further evidenced Congressional intent to draw FISA pen register law in accord with criminal law principles found in Title III and the ECPA.

[Redacted] section 1842(c) was amended to remove the requirement that the communication instrument had to be used to contact a foreign power or an agent thereof as a predicate to pen register authority. In explaining this amendment, Congress made clear its intent to conform FISA pen register authority to corresponding criminal law provisions:

b5

[This amendment] amends [the FISA pen register and trap and trace provisions] to mirror similar provisions that currently exist in criminal law (18 U.S.C. 3121 *et. seq.*) Currently, the "pen register and trap and trace" provisions of FISA go beyond the criminal law requirement of certification of relevance, and require that the communication instrument (*e.g.*, a telephone line) has been used to contact a "foreign power" or agent of a foreign power. This is a greater burden than exists in even a minor criminal investigation. [This amendment] clarifies that an application for pen register and trap and trace authority under FISA will be the same as the pen register and trap and trace authority defined in the criminal law.

House Report No. 107-236(I) *accompanying* Pub. L. 107-56 (October 11, 2001).

Congress went on later in the report to summarize its intent with regard to this amendment by stating "[t]he current statutory burden of having to show that the telephone line has been, or is about to be used to contact a foreign power or terrorist is eliminated to conform to the existing and less burdensome criminal standards." *Id.*

<sup>4</sup> Pub. L. 107-56; 115 Stat. 290 (October 26, 2001)

[Redacted]

b5

Second, Congress amended the definitions of pen register and trap and trace found at 18 U.S.C. 3127 (3), (4).<sup>6</sup> Those amendments, in part, struck out "electronic or other impulses which identify the numbers dialed..." and inserted "dialing, routing, addressing or signaling information...provided, however, that such information shall not include the contents of any communication..."

[Redacted]

b5

Lastly, Congress expressly imported into the definitional section of 18 U.S.C. 3127 (1) the definition of "contents" found in 18 U.S.C. 2510(8). As noted earlier in text, that definition was amended in 1986 to reflect the decisions of the Supreme Court in *New York Telephone and Smith v. Maryland* by deleting the identity of the parties or the existence of the communication.

[Redacted]

b5

[Redacted]

b5

**VIII. Rules of Statutory Construction**

When the terms of a statute are unambiguous, judicial inquiry is complete. *See, e.g., TVA v. Hill*, 437 U.S. 153, 187, n. 33 (1978); *Crooks v. Harrelson*, 282 U.S. 55 (1930). Moreover, the Supreme Court has warned against using the views of a later Congress to construe a statute enacted many years before. *See Pension Benefit Guaranty Corporation v. LTV Corp.*, 496 U.S. 633 (1990). It is, says the Court, "hazardous" to use later history as a basis to infer the intent of an earlier Congress and such views have "very little, if any, significance." *United States v. Price*, 361 U.S. 304, 313 (1960).

[Redacted]

b5

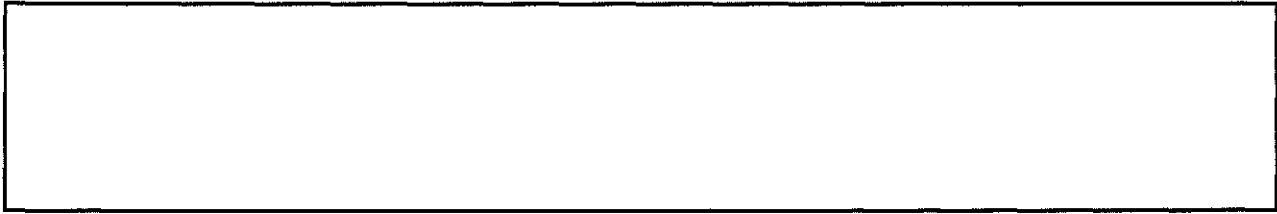
**IX. Conclusion**

[Redacted]

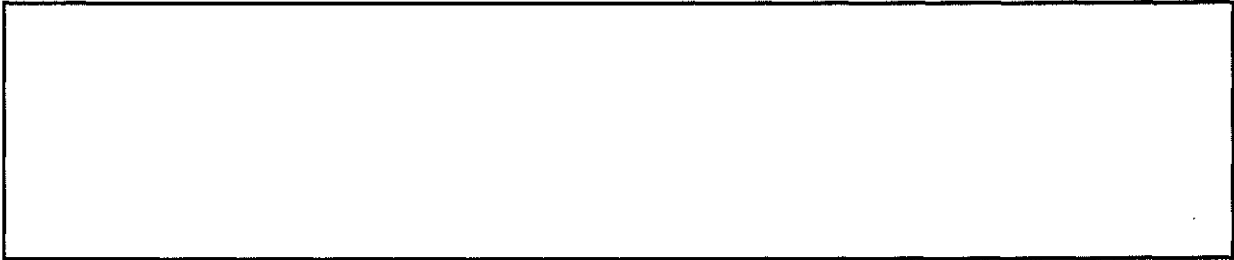
b5



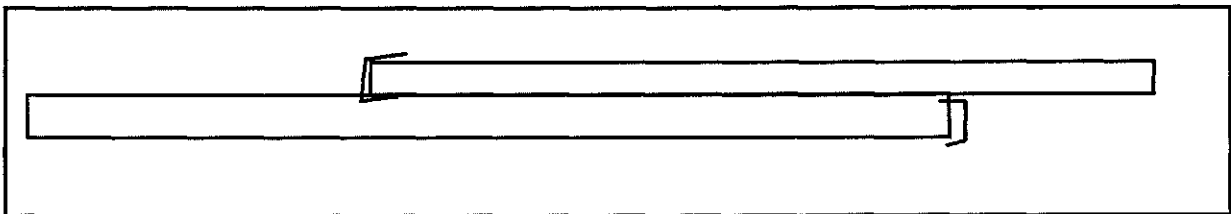
~~SECRET~~



b5



b5



(S)

b1  
b5

~~SECRET~~



Home  
Case

**Document** Index Lead Search Help  
Logout  
**View**  
Upload

b6  
b7C

## Document Details:

Return to Lead Summary List

Case ID:	66F-HQ-A1012493	Serial:	561
	66F-HQ-C1384970		19499
Ref Case ID:		Ref Serial:	
Office:	DP	Type:	EC
Date:	05/01/2005		
To:	ALL FIELD OFFICES COUNTERINTELLIGENCE COUNTERTERRORISM CRIMINAL INVESTIGATIVE CYBER GENERAL COUNSEL	From:	OPERATIONAL TECHNOLOGY
Author:		Approver:	
Topic:	TO REITERATE POLICIES AND PROCEDURES FOR REQUESTING		
Classification:	U		
Authority:		Duration:	
SCI Flag:		Rule(6e):	
IRS Tax:		Handling	
		Caveats:	
Secure document:			

b2



----- Document Text -----

Precedence: ROUTINE

Date: 05/01/2005

To: Cyber	Attn: Assistant Director
Counterintelligence	Attn: Assistant Director
Counterterrorism	Attn: Assistant Director
Criminal Investigative	Attn: Assistant Director
General Counsel	Attn: General Counsel
All Field Offices	Attn: ADIC, SAC, ASACs
	CDC
	Cyber SSAs
	Technical SSAs
	Technical Advisors
	Cyber SAs
	Technically Trained SAs
	FBIHQ, Manuals Desk

From: Operational Technology Division  
Data Intercept Technology Unit

Contact: SSA [Redacted]

Approved By: [Redacted]

Thomas Marcus C

[Redacted]

[Redacted]

b2  
b6  
b7C

Drafted By: [Redacted]

Case ID #: 66F-HQ-1012493 (Pending)

66F-HQ-C1384970 (Pending)

Title: DATA INTERCEPT TECHNOLOGY UNIT  
ADMINISTRATIVE  
POLICY MATTERS

Synopsis: To reiterate policies and procedures for requesting

and using Pen Register and Trap and Trace devices in FBI investigations.

Details: The policies and procedures set forth in MIOG, Part 2, 10-3, 10-10.7, 10-11.3 and 16-7.4.6 regarding the manner in which the use of the Pen Register and Trap and Trace techniques are to be requested, the approval levels, pertinent ELSUR procedures, and reporting requirements for the use of the Pen Register and Trap and Trace techniques apply to both the traditional telephonic Pen Registers (land line and cellular telephones) as well as to the more recently available use of the Pen Register and Trap and Trace technique, to capture "routing and addressing" information that identifies the sender or recipient of communications in a computer network or Internet environment.

The use of Pen Registers and Trap and Trace (Pen/Trap) devices allows the FBI to trace communications on the Internet and other computer networks. Orders issued by federal courts have nationwide effect. The Electronic Communications Privacy Act of 1986 (Act), as amended, regulates the use of a device to obtain any non-content information, including all dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications. The Act codifies existing Department of Justice (DOJ) policy of obtaining a court order to authorize the installation and use of a Pen Register and sets forth the procedure for seeking such an order.

A Pen Register in a computer network environment records or decodes routing and addressing information, which includes source and destination IP addresses, port numbers, "To:" and "From:" email account names, and other non-content information. The subject line of an email is considered to be content and is not captured under a Pen Register or Trap and Trace order.

[REDACTED]

b2  
b7E

On determining that the information likely to be

derived from a Pen Register/Trap and Trace (PR/TT) [redacted]

b2  
b7E

[redacted] the Case Agent should review applicable guidance in the MIOG. The policies and procedures relating to the technical aspects of requesting and using the technique are briefly reiterated below.

[redacted]

b2  
b7E

[redacted]

b2  
b7E

Field Supervisory personnel are to ensure that the use of the PR/TT is not substituted for other logical investigations. Prior to requesting that an attorney for the government apply for a PR/TT order under the Act, the Case Agent should submit an EC or other appropriate communication, initialed by the supervisor, to the case file and to the PR/TT control file setting forth the

reasons for PR/TT use and documenting the basis for the statements to be made in the application. If the United States Attorney or Strike Force Chief requires a written request specifying the factual basis for the assertions in the application, copies of the letter may be designated to the above-indicated files in lieu of a separate EC. The above instructions apply to all instances wherein a PR/TT is to be used, whether alone or in conjunction with the interception of wire or electronic communications under the provisions of the Act. The Chief Division Counsel (CDC) should be consulted if there is any question as to the sufficiency of facts stated or whether the existing facts are stated in a manner which would clearly warrant the assertions made in the application for the order. A copy of each order obtained must be filed in the PR/TT control file. MIOG Part 2, Section 10-10.7 (3)â

The TTA is responsible for ensuring that proper authority has been obtained for technical equipment use and maintaining a file which contains the documented authority (court orders, SAC or supervisory approval). The TTA will not permit the use of technical equipment until such court or other authority has been seen or orally verified from supervisory personnel. Such oral verification of court authority will be documented and maintained in the file with the court orders. MIOG PII 16-7.3.1

The nature of the Internet Service Provider community is such that a Case Agent may seek an order in his/her Division, the order may be served by an Agent or IA at the Provider's corporate presence in another Division, and the Pen Register may be installed in a third Division. This necessitates effective communication and assistance across Divisional boundaries. In furtherance of its mission, [REDACTED]

[REDACTED]

[REDACTED] for all methods of data network communications. DITU also provides coordination of technical issues associated [REDACTED]

b2  
b7E

[Redacted]

b2  
b7E

[Redacted] DITU provides technical assistance to the Field Office's Technical Investigative Program (TIP) for all aspects of the data network collection, from coordinating and installing the necessary equipment to providing software and training to aid in the processing and viewing of collected data. In addition, DITU is an authoritative source of information regarding current capabilities, procedures, and contact information [Redacted]

[Redacted]

b2  
b7E

[Redacted]

There have been instances in which Case Agents have approached Internet Service Providers directly and sought the provider's assistance in developing/executing Pen Register or electronic surveillance capability. In some of these instances, a capability already existed but the employee of the service provider with whom the Case Agent was communicating was unaware that the company had a nationwide capability in place. Needless delay in the execution of orders or added cost to the company and the FBI may result. Case Agents should coordinate any approach to an ISP for electronic surveillance-related matters with the Division TA/TTAs. [Redacted]

[Redacted]

b2  
b7E

[Redacted]

A change to the Pen Register statute with passage of the Patriot Act also included additional reporting as follows: If a law enforcement agency installs and uses its own Pen/Trap device on a packet-switched data network of a provider of electronic communication service to the public, the law enforcement agency must report the following information to the court ex parte and under seal within 30 days after termination of the order (including any extensions thereof): (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any

modifications to that configuration; and (4) the information collected by the device. (Title 18, USC, Section 3123(a)(3)) Systems developed by OTD/DITU to effect Pen Registers in computer networks contain features to automate as much of this reporting as possible but written logs and other documentation are still required by the Division's TA/TTA and Case Agent to comply with this statutory requirement.

The Act further requires that the Attorney General make an annual report to Congress on the number of Pen Register orders applied for by law enforcement agencies of the Department. DOJ has advised the FBI by memorandum of this requirement and has requested quarterly reports on Pen Register usage. Court-ordered Pen Register usage must be reported to FBIHQ within five workdays of the expiration date of any original or renewal order. To satisfy DOJ data requirements and standardize and simplify field reporting, use the FBI macro form number FD-712, captioned "Pen Register/Trap and Trace Usage." If an order is obtained, but no actual coverage of any lines is effected, then no submission is required. These reporting requirements do not apply to Pen Register usage effected under the provisions of the Foreign Intelligence Surveillance Act.



LEAD(s) :

Set Lead 1: (Info)

ALL RECEIVING OFFICES

Read and Clear.

----- Document Text -----

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 06/19/02

To: All Divisions

Attn: Assistant Director;  
SAC;  
Legat  
CDC

From: Office of the General Counsel  
Investigative Law Unit, Room 7326  
Contact: Investigative Law Unit, (202)324-5640

Approved By:



b6  
b7C

Drafted By:



*Serial 57*

Case ID #: 66F-HQ- 1085160(Pending)

Title: NEW LEGISLATION  
PATRIOT ACT OF 2001  
PROVISIONS ADDRESSING INVESTIGATIVE ISSUES

Synopsis: To supplement guidance previously provided on the USA PATRIOT ACT of 2001 by highlighting provisions of the USA PATRIOT Act of 2001 which are of the most immediate interest to FBI investigations.

Reference: 66F-HQ-A1247863 Serial 70  
66F-HQ-A1247863 Serial 71  
66F-HQ-A1323588 Serial 364

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (otherwise referred to as the "USA PATRIOT Act" or "Patriot Act") which enhances many investigative tools available to the FBI. Over the last several months, the Office of the General Counsel (OGC) has provided guidance to the field on this Act in the form of e-mails, L.O.s, and presentations/training. Among the documents provided are a detailed section-by-

To: All Divisions From: Office of the General Counsel  
Re: 66F-HQ-1085160, 06/19/2002

Best Available  
Copy

section analysis of certain provisions of the Act;<sup>1</sup> two separate ECs prepared by OGC's National Security Law Unit [redacted]

[redacted]

b5

[redacted] The purpose of this communication is to consolidate into one document the guidance previously provided and to highlight those provisions of the Patriot Act of greatest interest to FBI investigative efforts.

[redacted]

b5

[redacted]

b5

[redacted]

[redacted]

b5

I. Investigative Tools

[Redacted]

b5

[Redacted]

b5

[Redacted]

b5

[Redacted]

b5

[Redacted]

b5

[Redacted]

b5

To: All Divisions From: Office of the General Counsel  
Re: 66F-HQ-1085160, 06/19/2002

[Redacted]

b5

[Redacted]

[Redacted]

b5

[Redacted]

b5

[Redacted]

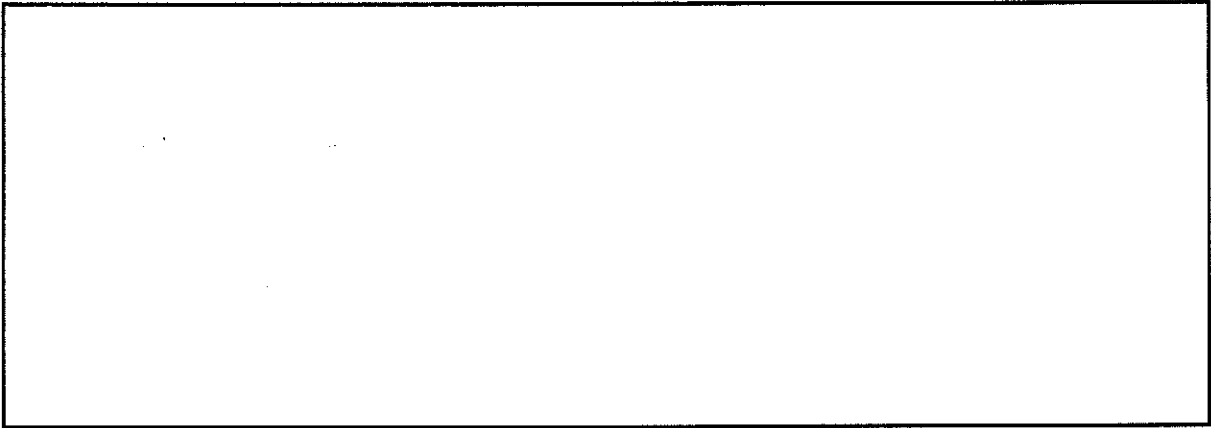
b5

[Redacted]

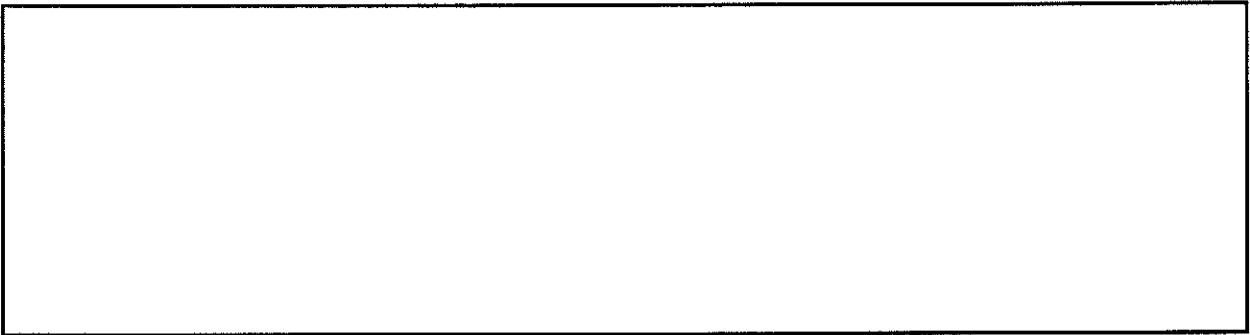
[Redacted]

b5

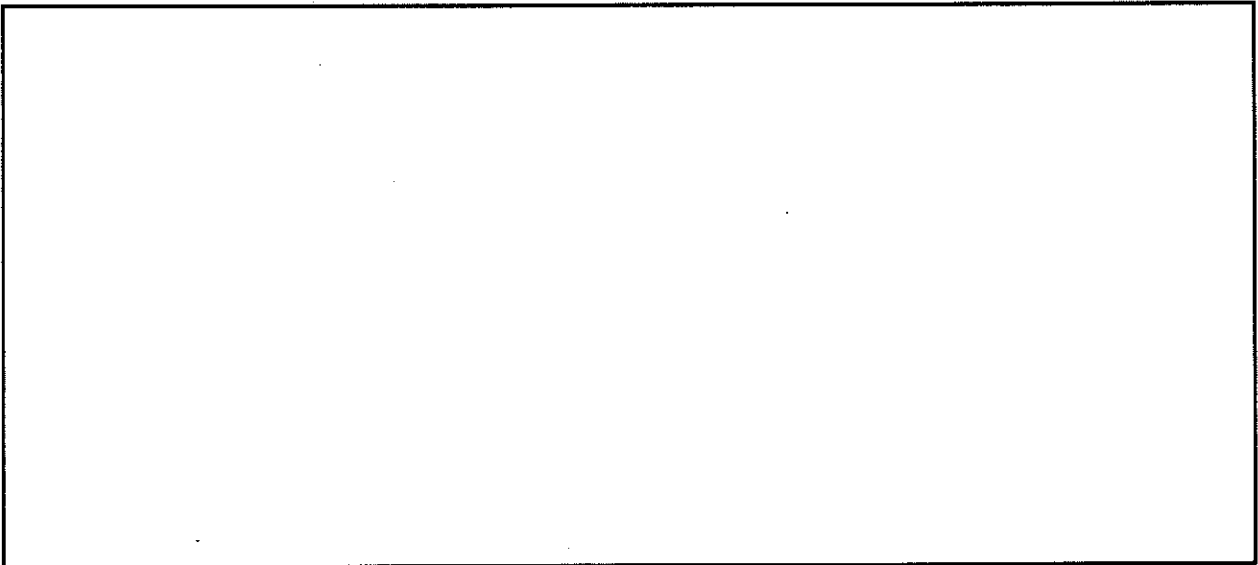
To: All Divisions From: Office of the General Counsel  
Re: 06F-HQ-1085160, 06/19/2002



b5



b5



b5

[Redacted] (OTD) (FBI)

From: [Redacted] (OTD) (FBI) b6  
Sent: Tuesday, March 18, 2008 3:20 PM b7c  
To: [Redacted] (OGC) (FBI)  
Cc: [Redacted] (OTD) (FBI)  
Subject: RE: PR/TT annual report

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

[Redacted]

b6  
b7c

I have been sending a quarterly report and the annual report to the DOJ on the FBI's Pen Register and Trap and Trace usage since I came into this position 22 years ago. I have a copy of a memorandum from William F. Weld, Assistant Attorney General, DOJ dated 01/15/1987, instructing the Bureau to report Trap and Trace usage to the DOJ on a quarterly basis. (I do not have any of the documentation that initially required the Bureau to report the Pen Register Usage. However, those reports were being generated when I assumed the position.) I also have a copy of a memorandum from Frederick D. Hess, Director, Office of Enforcement Operations, Criminal Division, DOJ, dated 11/24/1987, that instructs us to report on an annual basis, in a different format, the Pen Register and Trap and Trace statistics. This memorandum advises that the information detailed in the annual report is then reported to congress. We have been preparing both reports (based on information from the field offices, submitted via the FD-712), in the same manner since that time. Since the receipt of the two referenced memorandums, I have not been advised of any additional direction or changes from the DOJ.

[Redacted]

b6  
b7c

From: [Redacted] (OGC) (FBI)  
Sent: Tuesday, March 18, 2008 2:47 PM b6  
To: [Redacted] (OTD) (FBI) b7c  
Cc: [Redacted] (OTD) (FBI)  
Subject: PR/TT annual report

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

[Redacted]

b6  
b7c

I understand that you have been the one preparing our annual report to DOJ on PR/TT usage. Have you received any specific guidance or requirements from DOJ for this, or is this one of those items that we just report every year without a specific request? Thanks,

[Redacted]

b6  
b7c

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Best Available Copy  
**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/12/2000

To: All Field Offices

Attn: SACs  
Technical Advisors  
Technical Supervisors

Criminal Investigative  
Laboratory

[Redacted] Rm 5155  
[Redacted] QT-ERF  
[Redacted] QT-ERF  
[Redacted] QT-ERF  
[Redacted] QT-ERF

b6  
b7C

From: Laboratory  
Technical Operation Section/TICTU/QT-ERF  
Contact: [Redacted]

b6  
b7C

Approved By:

[Redacted Signature]

b6  
b7C

Drafted By:

[Redacted Name]

ehk [Signature] b6  
b7C

Case ID #: 66-HQ-19235-08007

Title: PEN REGISTER REPORTS

Synopsis: All FBI field offices are required to submit FD-712, Pen Register and Trap/Trace Usage reports within five workdays of the expiration date of any original or renewal order.

Details: In accordance with MIOG, Part II, Section 10-10.7, and the Electronic Communications Privacy Act of 1986 (ACT), Title 18, USC, Sections 3121-3127, the Laboratory Division (LD), Technical Operations Section (TOS), Telecommunications Intercept and Collection Technology Unit (TICTU), is required to report to the Department of Justice (DOJ), on a quarterly basis, the number of pen registers and trap and trace orders obtained by the FBI. To facilitate the DOJ reporting requirement and to standardize and simplify the field reporting, the FD-712, Pen Register and Trap/Trace Usage form was created and has recently been modified. The proper FD-712 form to be used is dated 01/18/2000. The MIOG, Part II, Section 10-10.7(4) stipulates that this form must be completed and submitted to FBIHQ within five workdays of the expiration date of any original or renewal order.

UPLOADED

FD-712 wpd

MAY 13 2000

S.D.J.



To: All Field Offices From: Laboratory  
Re: 66-HQ-19235, 05/12/2000

Best Available Copy

In addition to satisfying DOJ reporting requirements, the information received on the FD-712 is analyzed by TICTU and the Criminal Investigative Division to determine the alignment and allocation of human, fiscal, and electronic surveillance equipment resources. This information is also used to justify the procurement of electronic surveillance equipment and out-year budget enhancement requests.

Failure to provide prompt and accurate information on the FD-712 is in violation of the MIOG and may result in inadequate resources available to support critical electronic surveillance requirements.

To: All Field Offices From: Laboratory  
Re: 66-HQ-19235, 05/12/2000

Best Available Copy

LEAD(s) :

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

All FBI field offices are to ensure that the FD-712, Pen Register and Trap/Trace Usage Reports are submitted to the LD, TOS, TICTU in accordance with MIOG, Part II, Section 10-10.7.

♦♦

Best Available Copy

(Rev. 01-31-2003)

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 04/25/2006

To: All Field Offices

Attn: ADIC, SACs, ASACs,  
CDCs  
Technical Supervisors  
Technical Advisors  
ELSUR Technicians

General Counsel  
Operational Technology  
Records Management

Attn: [REDACTED]  
Attn: [REDACTED] TICTU  
Attn: [REDACTED] PPU  
Forms Desk  
Manuals Desk

STLU b6  
b7C

From: Operational Technology  
DES/Data Intercept Technology Unit  
Contact: [REDACTED]

b6  
b7C

Approved By: [REDACTED]

b6  
b7C

Drafted By: [REDACTED]

:glm

b6  
b7C

Case ID #: 319W3-HQ-A1487699-OTD (Pending)

Title: PROCEDURAL AND OPERATIONAL ISSUANCES  
DATA INTERCEPT TECHNOLOGY UNIT (DITU)  
POLICY MATTERS  
PEN REGISTER/TRAP AND TRACE REPORTING REQUIREMENTS

Synopsis: To reiterate reporting requirements for the use of the Pen Register/Trap and Trace investigative technique.

Reference: 66F-HQ-1092598 SUB F Serial 11  
66F-HQ-1012493 SUB F Serial 22  
HQ 66-A19235 Serial 51826 and 62011  
66F-HQ-C1384970 Serial 15883

Enclosure(s): Enclosed for Records Management Division, PPU, Forms Desk is a recommended version of the FD-712.

Details: The FBI has a reporting requirement associated with the use of Pen Register/Trap and Trace devices as set out in Title 18 U.S.C., section 3126, as implemented by MIOG, Part II, Section 12-16.7. The Pen Register statute requires the Attorney General to make an annual report to Congress on the number of pen

To: All Field Offices From: Operational Technology  
Re: 319W3-HQ-A1487699-OTD, 04/25/2006

register orders applied for by law enforcement agencies of the Department of Justice (DOJ). The DOJ has advised the FBI by memorandum of this requirement and has requested quarterly reports on pen register/trap and trace usage. To comply with this requirement, MIOG 10-10.7(5) states in part that court-ordered pen register usage must be reported to FBIHQ within five workdays of the expiration date of any original or renewal order. To satisfy DOJ data requirements, and standardize and simplify field reporting, the MIOG directs use of FBI form number FD-712, captioned "Pen Register/Trap and Trace Usage." If an order is obtained, but no actual pen register or trap and trace coverage of telephone lines, Internet/network connections or e-mail accounts is effected, then no submission is required. These reporting requirements do not apply to pen register/trap and trace usage effected under the provisions of the Foreign Intelligence Surveillance Act.

Although the MIOG is silent on the assignment of responsibility for the timely filing of the FD-712, the case agent is frequently relieved of this administrative task by the ELSUR Technician, who in most instances files the FD-712 on the expiration of an original or renewal order. Regardless, the case agent remains responsible for this submission.

The FD-712 must contain the court order number, primary statutory citation, order expiration date, termination date, Judge and District granting authorization and the actual number and nature of facilities affected. The facility categories are landline, cellular, Internet/network and e-mail.

It should be noted that while the requirements listed in the paragraph above do fulfill the requirements of the FD-712, they do not fulfill those of the statute, Title 18 U.S.C. Section 3126, requiring the AG to report:

- 1) The period of interceptions authorized, and the number and duration of any extensions. (This information would be very difficult to obtain just from the FD-712.)
- 2) The offense specified in the order or application or extension.
- 3) The number of investigations involved. (The FD-712 has the serial number so it is possible for someone with access to ACS to obtain this information, however it would be difficult for others.)
- 4) The number and nature of the facilities affected,

To: All Field Offices From: Operational Technology  
Re: 319W3-HQ-A1487699-OTD, 04/25/2006

Best Available Copy

5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

To further confuse the issue, there are currently two versions of the FD-712, both containing the same revision date (08-28-2002). One is obtained from the WordPerfect FBI Macros drop-down menu. This version is the most recent and contains the fields necessary to report the judge and district granting authorization, and the number of Internet/network and e-mail intercepts. The other version is obtained from the forms link on the FBI intranet web site ([http://rmd.fbinet.fbi/fd forms/pdf forms/fd-712.pdf](http://rmd.fbinet.fbi/fd%20forms/pdf%20forms/fd-712.pdf)). This version does not contain these two fields. In order to report all the required information, it is requested that the WordPerfect macro version be utilized until such time as the forms link version is corrected.

b6  
b7c

Also, this form generates an EC which is addressed to [redacted] Technical Operations Section, Telecommunications Intercept and Collection Technology Unit (TICTU), Quantico ERF". These forms containing Internet/network or e-mail collections, must then be forwarded from the TICTU to the DITU. The DITU is then responsible for reporting this information to the DOJ.

The USA Patriot Act clarified that the Pen Register statute includes "routing and addressing" information as well as "dialed digits," thereby applying the Pen Register/Trap and Trace investigative technique to Internet communications. Title 18 U.S.C., Section 3123(a)(3) establishes a second reporting requirement for Pen Register/Trap and Trace collections. It states:

"(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify:

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time and duration of each time the device is accessed to obtain information;

Best Available Copy

To: All Field Offices From: Operational Technology  
Re: 319W3-HQ-A1487699-OTD, 04/25/2006

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

(iv) information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof)."

To accomplish this reporting requirement, whenever DITU installs a criminal data pen register, a text file will also be created by DITU on the collection computer. All the information required by 18 U.S.C., Section 3123(a)(3)(A)(i) through (iii) will be recorded in this text file. Upon termination of the pen register order, this text file will be provided to the case agent for submission to the court with the data required by (A)(iv).

To: All Field Offices From: Operational Technology  
Re: 319WB-HQ-A1487599-OTD, 04/25/2006

LEAD(s):

Set Lead 1: (Action)

RECORDS MANAGEMENT

AT WASHINGTON, DC

Update the FD-712 on the forms link web site to capture all information required by statute.

Set Lead 2: (Info)

ALL RECEIVING OFFICES

Read and clear.

♦♦

[Redacted]

b6  
b7C

From: [Redacted]

Sent: Monday, February 12, 2007 8:04 AM

To: [Redacted]

Cc: [Redacted]

b2  
b7E

b2  
b7D  
b7E  
b5

Subject: FW: CALEA [Redacted] and [Redacted]

b6  
b7C

b7D

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

b6  
b7C  
b7D  
b5

Please call me as soon as possible to discuss this matter. [Redacted]

[Redacted]

Deputy General Counsel  
Investigative Law Branch  
Office of the General Counsel  
Federal Bureau of Investigation

b6  
b7C

[Redacted]



### **How long can notice be delayed?**

- The most common period of delay authorized by courts is seven days. Courts have authorized specific delays of notification as short as one day and as long as 90 days; other courts have permitted delays of unspecified duration lasting until an indictment was unsealed.

### **PEN REGISTER/ TRAP AND TRACE/ ROVING SURVEILLANCE**

#### **How did the Patriot Act expand the FBI's electronic surveillance abilities?**

- Before the Patriot Act, many of our investigative tools did not account for new communications technologies like e-mail and cell phones, leaving gaps that terrorists could exploit. The Patriot Act made common-sense changes that adapted established authority to modern technology and the borderless nature of cyberspace.
- Before the Act, law enforcement could get court permission for a "roving wiretap" to track a drug dealer who switched from one cell phone to another, but we could not get a similar authority to track terrorists. Now we can. The Patriot Act simply amended the Foreign Intelligence Surveillance Act to conform to the parallel provision found in the Federal Wiretap Statute.
- Section 216 of the Patriot Act amends the pen register/trap and trace statute to clarify that it applies to Internet communications, and gives federal courts authority to authorize the installation and use of pen registers and trap and trace devices in other districts.

#### **What is meant by pen register/trap and trace?**

- The so-called pen register/trap and trace statute allows us to collect non-content information about a communication, such as the numbers dialed to or from a telephone. The Patriot Act updated this statute to account for Internet communications by allowing us to collect subscriber informational headings.
- In order to get access to the content of Internet communications, we still need to make a full showing under Title III or FISA.

#### **Did the Patriot Act change the standard for obtaining a pen register? What is the standard?**

- The Patriot Act did not change the standard needed to obtain a pen register. Under prior law, the government could obtain a pen register for a telephone by certifying that the information likely to be obtained was relevant to an ongoing investigation.

### **Does the Patriot Act allow the FBI to go "fishing" through my e-mail?**

- Fishing expeditions of people's e-mail messages are not permitted.
- The Patriot Act permits a judge to enter a pen register order allowing the government to obtain addressing and routing information - the addresses of e-mail messages. The order does not permit the interception of content, including the subject line of an e-mail message.
- Before a court will enter a pen register order, a government attorney must certify that the information is relevant to an ongoing criminal investigation, or, in a foreign intelligence case, that the information is relevant to an investigation to protect against international terrorism or clandestine intelligence activities or to obtain foreign intelligence information not concerning U.S. persons (defined as citizens and permanent resident aliens).

### **How has the FBI's used its new pen register/trap and trace authority?**

- These tools have helped us track the communications of terrorist conspirators and proved critical to identifying some of those involved in

b2  
b7E

### **Won't use of the new pen register/trap and trace authority violate the privacy rights of Internet users?**

- No. This authority only permits us to look at addressing information, not the contents of e-mails, and there are strict constraints on its use.
- Pen registers and trap and trace devices are investigative tools that have been available to law enforcement for years for use on telephone calls. Before the Patriot Act, judges had applied the telephone rules to e-mail as well as telephones, but the rules were not uniform across the country. The Patriot Act simply makes it clear that the same uniform rules that apply to telephone calls also apply to e-mail.

### **What is a "roving" wiretap?**

- Roving wiretaps allow a wiretap order to be specific to a person, regardless of which telephone he is using, rather than specific to a particular telephone. This makes sense because an individual could easily use multiple telephones.
- Section 206 of the Patriot Act extended to foreign intelligence investigations the same ability to obtain a roving wiretap that has existed for years in criminal investigations.

109th CONGRESS

1st Session

**S. 737**

To amend the USA PATRIOT ACT to place reasonable limitations on the use of surveillance and the issuance of search warrants, and for other purposes.

**IN THE SENATE OF THE UNITED STATES**

April 6, 2005

Mr. CRAIG (for himself, Mr. DURBIN, Mr. SUNUNU, Mr. FEINGOLD, Ms. MURKOWSKI, and Mr. SALAZAR) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

**A BILL**

To amend the USA PATRIOT ACT to place reasonable limitations on the use of surveillance and the issuance of search warrants, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE.**

This Act may be cited as the 'Security and Freedom Enhancement Act of 2005' or the 'SAFE Act'.

**SEC. 2. LIMITATIONS ON ROVING WIRETAPS UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.**

Section 105(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)) is amended--

(1) in paragraph (1), by striking subparagraphs (A) and (B) and inserting the following:

(A)(i) the identity of the target of the electronic surveillance, if known; or

(ii) if the identity of the target is not known, a description of the target and the nature and location of the facilities and places at which the electronic surveillance will be directed;

`(z) Aggrieved Person- The term `aggrieved person' means any consumer or person whose consumer report is produced, disclosed, or otherwise made public without the consent of such consumer or person.

`(aa) Foreign Power- The term `foreign power' has the meaning given such term by section 101(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(a)).'.

## SEC. 6. PRIVACY PROTECTIONS FOR PEN REGISTERS AND TRAP AND TRACE DEVICES.

### (a) Criminal Authority-

(1) APPLICATION FOR AN ORDER- Section 3122(b)(2) of title 18, United States Code, is amended by striking `a certification by the applicant' and inserting `a statement by the applicant of specific and articulable facts showing there is reason to believe'.

(2) ISSUANCE OF AN ORDER- Section 3123(a) of title 18, United States Code, is amended--

(A) in paragraph (1), by striking `the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.' and inserting `the application meets the requirements of section 3122.'; and

(B) in paragraph (2), by striking `the State law enforcement or investigative officer' and all that follows and inserting `the application meets the requirements of section 3122.'.

(3) REPORTING- Section 3126 of title 18, United States Code, is amended--

(A) in the matter preceding paragraph (1), by striking `law enforcement agencies of the Department of Justice' and inserting `attorneys for the Government';

(B) in paragraph (4), by striking `and' at the end;

(C) in paragraph (5), by striking the period and inserting `; and';

(D) in the matter preceding paragraph (1), by striking `The Attorney General' and inserting the following:

`(a) Report to Congress- The Attorney General'; and

(E) by adding at the end the following:

` (6) whether the application for the order and the applications for any extensions were granted as applied for, modified, or denied;

` (7) the specific types of dialing, routing, addressing, or signaling information sought in the application and obtained with the order; and

` (8) a summary of any litigation to which the Government is or was a party regarding the interpretation of the provisions of this chapter.

` (b) Public Report- The Attorney General shall annually make public a full and complete report concerning the number of applications for pen register orders and orders for trap and trace devices applied for pursuant to this chapter and the number of such orders and extensions of such orders granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be reported to Congress under subsection (a).'

(4) NOTICE- Section 3123 of title 18, United States Code, is amended by adding at the end the following:

` (e) Notice-

` (1) INVENTORY- A court that receives an application for an order or extension under section 3122(a) shall cause to be served on the persons named in the application, and such other parties to communications as the court determines should receive notice in the interest of justice, an inventory, including--

` (A) the fact of the application for an order or extension under section 3122(a) and whether the court granted or denied such application; and

` (B) if the order or extension was granted--

` (i) the date of the entry of such order or extension and the period of authorized, approved, or disapproved use of the pen register or trap and trace device;

` (ii) whether a pen register or trap and trace device was installed or used during the period authorized; and

` (iii) the specific types of dialing, routing, addressing, or signaling information sought in the application and collected by the pen register or trap and trace device.

` (2) TIMING- The court shall serve notice under paragraph (1) within a reasonable time, but not later than 90 days after--

` (A) the filing of the application for an order or extension under section 3122(a) that is denied; or

`(B) the termination of the period of an order, or extensions thereof, that is granted.

`(3) DELAY- The court may issue an ex parte order postponing the service of the inventory required under paragraph (1) upon a showing of good cause by an attorney for the Government.

`(4) INSPECTION- Upon the filing of a motion, the court may make available for inspection by a person served under paragraph (1), or counsel for such person, such portions of the collected communications, applications, and orders as the court determines to be in the interest of justice.'.

(b) Foreign Intelligence Authority- Section 402(c)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842(c)(2)) is amended by striking `a certification by the applicant' and inserting `a statement by the applicant of specific and articulable facts showing there is reason to believe'.

#### SEC. 7. MODIFICATION OF DEFINITION OF DOMESTIC TERRORISM.

Section 2331(5) of title 18, United States Code, is amended--

(1) by striking subparagraphs (A) and (B) and inserting the following:

`(A) involve acts dangerous to human life that constitute a Federal crime of terrorism (as that term is defined in section 2332b(g)(5)); and'; and

(2) by redesignating subparagraph (C) as subparagraph (B).

#### SEC. 8. PUBLIC REPORTING ON THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) In General- Section 601(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(a)) is amended in the matter preceding paragraph (1)-

(1) by striking `, in a manner consistent with the protection of national security,'; and

(2) by inserting `public' before `report'.

(b) Redaction- Section 601(a)(5) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(a)(5)) is amended by inserting `, which may be redacted in order to protect national security' after `that include significant construction or interpretation of the provisions of this Act'.

**SEC. 2. PATRIOT SECTIONS 203; COURT NOTICE**

- [Redacted]
- [Redacted]
- [Redacted]

**SEC. 3. PATRIOT SECTION 206; ROVING**

(a) PARTICULARITY REQUIREMENT

- [Redacted]
- [Redacted]

(b) ADDITIONAL DIRECTIONS

- [Redacted]
- [Redacted]

(c) ENHANCED OVERSIGHT

**SEC. 4. PATRIOT SECTION 207; DURATION**

**SEC. 5. PATRIOT SECTION 212; EMERGENCY DISCLOSURES**

(a) ENHANCED OVERSIGHT (our reporting requirement)

(b) TECHNICAL AMENDMENTS

- [Redacted]

**SEC. 6. PATRIOT SECTION 213; DELAYED NOTICE SEARCH WARRANTS**

(a) GROUNDS FOR DELAY & (b) REASONABLE PERIOD OF DELAY

- [Redacted]

(c) ENHANCED OVERSIGHT

- [Redacted]
- [Redacted]
- [Redacted]

**SEC. 7. PATRIOT SECTION 214; FISA PEN REGISTER AND TRAP AND TRACE AUTHORITY**

(a) FACTUAL BASIS

- [Redacted]

(b) RECORDS (SSCI fix)

(c) ENHANCED OVERSIGHT

- [Redacted]

**SEC. 8. PATRIOT SECTION 215; FISA BUSINESS RECORDS**

(a) FACTUAL BASIS

- [Redacted]

(b) ADDITIONAL PROTECTIONS

- [Redacted]
- [Redacted]

(c) DIRECTOR APPROVAL

- [Redacted]

(d) PROHIBITION ON DISCLOSURE

- [REDACTED]
- [REDACTED]
- (e) JUDICIAL REVIEW  
• [REDACTED]
- (f) ENHANCED OVERSIGHT  
• [REDACTED]

**SEC. 9. NSLs**

**SEC. 10. SUNSET PROVISIONS**

- [REDACTED]

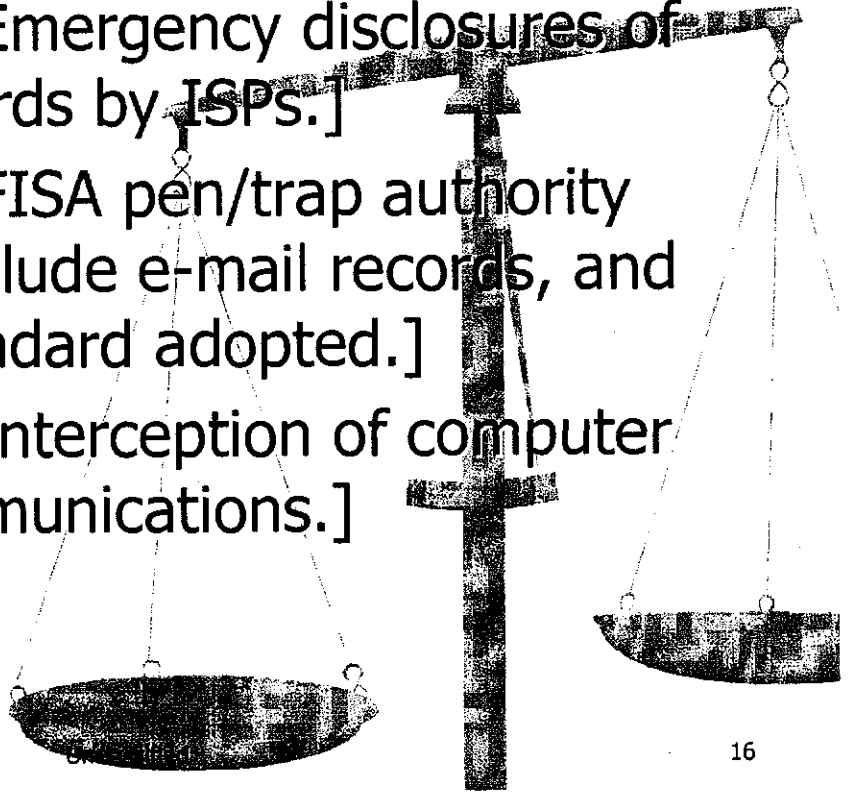
**SEC. 11. ENHANCEMENT OF SUNSHINE PROVISIONS**

- [REDACTED]



# USA PATRIOT Act 2001 Sunset Provisions - Permanent

- **Section 212** [Emergency disclosures of e-mail and records by ISPs.]
- **Section 214** [FISA pen/trap authority expanded to include e-mail records, and "relevance" standard adopted.]
- **Section 217** [Interception of computer trespasser communications.]



[redacted] (RMD) (FBI)

b6  
b7C

From: [redacted] (OGC) (FBI)  
Sent: Thursday, August 23, 2007 6:19 PM  
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted]  
Subject: [redacted] (OGC) (FBI)  
RE: FBI SES Call to Prepare Appraisal Input

UNCLASSIFIED  
NON-RECORD

Here's a bit more than a bullet on the J-STD-025-B petition, but some background might be warranted here:

The Communications Assistance for Law Enforcement Act (CALEA) maintains law enforcement's ability to continue to conduct lawfully-authorized electronic surveillance (LAES) despite technological changes by further defining the telecommunications industry's existing obligation to provision LAES, and requires industry to develop and deploy CALEA intercept solutions in their networks to ensure that LAES can be performed. Among other things, CALEA explicitly obligates telecommunications carriers to ensure that their equipment, facilities, and services are capable of isolating and delivering to law enforcement all call-identifying information and call content to which it is legally entitled in a manner that allows it to be associated with the communication to which it pertains. CALEA sets forth general assistance capability requirements, but contemplates that the communications industry — acting in consultation with law enforcement — will develop standards that meet the assistance capability requirements of the statute. If an industry-adopted standard does not meet CALEA's mandate, CALEA permits the government or others to file a deficiency petition with the Federal Communications Commission (FCC) requesting the establishment by rule of modified or additional requirements/standards.

b2  
b7E

J-STD-025-B is the industry-adopted CALEA standard for LAES [redacted]

[redacted] A number of carriers — most significantly [redacted] and [redacted] who collectively have over 100 million customers — have deployed CALEA solutions based on J-STD-025-B. Unfortunately, solutions based on J-STD-025-B fail to meet the assistance capability requirements of CALEA because they do not include certain capabilities, specifically [redacted]

[redacted]

[redacted] In an effort to resolve the problems in J-STD-025-B, FBI — together with DOJ's Criminal and National Security Divisions and DEA — filed a comprehensive deficiency petition with the FCC in May, 2007 requesting that the FCC adopt rules requiring carriers to provide the above-referenced capabilities. The FCC has since solicited public comment from industry and other interested parties on the petition, and it is expected that the FCC will in the near term issue a comprehensive Notice of Proposed Rulemaking with its tentative conclusions for resolving the issues raised in the petition concerning the missing capabilities.