

DOJ's Patriot Act Talking Points	Patriot Act Reality
---	----------------------------

<p>SECTION 505 OF THE PATRIOT ACT (AND THE INTELLIGENCE BILL) EXPANDED THE POWER OF THE FBI TO ISSUE NATIONAL SECURITY LETTERS (NSLS), WHICH APPLY TO CREDIT REPORTS, ELECTRONIC COMMUNICATIONS SERVICE PROVIDER (ISP) RECORDS, AND FINANCIAL RECORDS</p> <p>[Background: These provisions expanded the power of the FBI to issue NSLs to a wider array of American businesses and eliminated the requirement that there be specific and articulable facts connecting the records sought to a suspected terrorist. A “financial institution” is defined to include banks, credit companies, insurance companies, car dealerships, jewelers, hotel-casinos, travel agencies, and real estate closing firms, among others. The FBI has interpreted ISPs to include businesses that provide internet access for patrons or customers. Last year almost 10,000 (9254) NSLS were issued by the FBI.]</p> <p>Rhetoric: The conference report ... permits disclosure to legal counsel. ... creates explicit right to judicial review. “if compliance would be unreasonable, oppressive, or otherwise unlawful.” ... permits judicial review of non-disclosure requirement of NSLs. ... requires the court to treat the Government’s certification that disclosure “may endanger the national security of the United States” ... as “conclusive” unless made in “bad faith,” but requires certification by only high ranking officials to get such deference. ... requires two IG audits of NSLs, retroactively and prospectively, and reporting of aggregate statistics and the feasibility of minimization procedures</p>	<p>Does <u>not</u> require court approval.</p> <p>Does <u>not</u> require any connection between the records and a suspected foreign terrorist. Patriot Act eliminated requirement that there be “specific and articulable” facts connecting records sought to a target, a suspected foreign terrorist.</p> <p>Illusory right to challenge secrecy. Non-disclosure orders accompany the NSLs and customers will never know their records were given to the FBI. Businesses can challenge secrecy, but the court must accept the government’s assertion of harm to national security, diplomatic relations, or criminal investigation as “conclusive.” This gives a “right” that is an illusion in practice because the challenger can never win under this “standard,” which is plainly unconstitutional. In an NSL case, the FBI used the ISP power to try to get computer records from a member of the American Library Association. The court examined the asserted basis for the gag and found it wanting. Under the new “standard” the court would not be able to do so unless ruling against the standard. (DOJ dropped its appeal of the gag.)</p> <p>Express right to consult lawyer.</p> <p>Right to challenge order. Recipient can challenge the order as unlawful, unreasonable or oppressive.</p> <p>Gives the government the power to enforce NSL as a subpoena.</p> <p>More study won’t protect our privacy. Plus, the statistics should have been made public long ago.</p>
--	---

DOJ's Patriot Act Talking Points	Patriot Act Reality
---	----------------------------

<p>SECTION 215 IS KNOWN AS THE “LIBRARY RECORDS” PROVISION, BUT IT APPLIES TO ANY TANGIBLE THING —MEDICAL, TAX, GUN AND OTHER RECORDS.</p> <p>[Background: This provision allows the federal government to get a secret court order for any records or other “tangible things” by certifying merely that they are “sought for” an authorized counter-intelligence, which the Justice Department says is the equivalent of “relevant to.” <u>Does not require</u> a connection between the records sought and a suspected terrorist. The Patriot Act eliminated the requirement that there be “specific and articulable” facts connecting records sought to a target of an intelligence investigation (a person there is probable cause to believe is an agent of a foreign power). Last year, the FISA Court approved 155 Section 215 orders for records.]</p> <p>Rhetoric: The conference report ... requires “a statement of facts” showing “reasonable grounds to believe” things sought are relevant to an authorized investigation to protect against international terrorism or espionage. ...[creates] a legal presumption in favor of records that pertain to a foreign power or an agent of a foreign power or someone “in contact with, or known to,” suspected agent of a foreign power. ... includes an explicit right to consult legal counsel and judicial review. ... requires FBI Director [or designee] to approve requests for certain records, including library, medical, educational, and tax records plus increased reporting ... requires minimization procedures to limit retention of info on US residents. ...requires two IG audits of Section 215 orders, retroactively and prospectively.</p>	<p><u>Does not require a connection between the records sought and a suspected terrorist.</u> Does not require that the records sought pertain to a terrorist organization, a suspected terrorist, or even someone conspiring or in contact with a suspected terrorist. Relevance to protect against terrorism is virtually meaningless. Adding a presumption of relevance does not require a connection and makes it easier to sweep in First Amendment protected activity. Without such requiring a connection this provision remains a license for fishing expeditions.</p> <p>Limited right to challenge order. The recipient can tell counsel and has a limited right to file a challenge to the order in the FISA court, to be heard by a specially pre-selected three-judge panel. The panel can only examine whether the order is authorized by Section 215 or is unlawful. After-the-fact challenge will not cure the failure to limit fishing expeditions into personal records of innocent people in the first place—many businesses won’t challenge.</p> <p>Illusory right to challenge secrecy. Same flawed standard as for NSLs.</p> <p>Express right to consult lawyer.</p> <p>The so-called “grand jury” limitation is meaningless. Provision makes clear that privileged information can be gather under 215.</p> <p>Punting to DOJ to create secret, unenforceable “minimization” rules won’t cure these failures.</p> <p>More study won’t protect privacy.</p>
---	--

<p><u>SUNSETS</u> THE PATRIOT ACT DESIGNATED 16 PROVISIONS TO EXPIRE ON DECEMBER 31, 2005 IF NOT REAUTHORIZED.</p> <p>[Background: The original Patriot Act had 16 provisions designated to sunset at the end of 2005.]</p> <p>The conference report retains 4-year sunsets for two of the most controversial PATRIOT Act provisions:</p> <p>Section 206, governing multi-point or "roving" wiretaps; and</p> <p>Section 215, governing court orders for business records in intelligence cases.</p> <p>It also puts a four-year sunset on the "Lo Wolf" provision added to the Foreign Intelligence Surveillance Act by last year's Intelligence Reform Act.</p>	<p>Extends sunsets for 4 years for 3 provisions. Makes almost all of the expiring provisions of the Patriot Act permanent. Extends the expiration date on Section 215 (FISA orders for personal records), Section 206 (John Doe roving wiretaps), and the lone wolf provision for 4 years.</p> <p>Four-year sunset. Would extend these powers for four years, for the rest of this administration. Bipartisan majorities in both houses favored a short four-year sunset.</p> <p>Does not cure substantive flaws. Even the shorter extension of unconstitutional powers will not cure the license to conduct fishing expeditions into innocent Americans' private records under Section 215. And, the new sunset dates have no impact on the even more troubling NSL powers, which were expanded by the Patriot Act and are permanent.</p>
--	---

DOJ's Patriot Act Talking Points	Patriot Act Reality
---	----------------------------

<p>SECTION 213, THE “SNEAK AND PEEK” POWER, CREATES A NATIONAL RIGHT FOR FEDERAL LAW ENFORCEMENT TO DELAY NOTICE OF SEARCH WARRANTS FOR HOMES OR BUSINESSES— NOT LIMITED TO TERRORISM CASES.</p> <p>[Background: Allows delayed notice searches of Americans’ homes or businesses for unspecified “reasonable time” where notice may cause specified harms (endanger life/physical safety; cause flight; cause loss of evidence; cause witness tampering) and gives a “catch-all” basis: if notice would “seriously jeopardize an investigation or unduly delay a trial.” Prior to the Patriot Act, only a few appellate courts had approved secret physical searches of people’s homes or businesses and only for short periods, mainly 7 days for extraordinary circumstances. No current report on number of 213 orders in 2005. There were 155 as of May 2005; most appear to have been used in drug cases, not terrorism.]</p> <p>Rhetoric: The conference report ... requires notice of the search to be given within <u>30 days</u> of its execution, unless the facts justify a later date certain. Although this period is a few weeks longer than the 7-day time limit in the original Senate bill, it is considerably shorter than the 180 days permitted under the House bill.</p> <p>... permits extensions of the delay, but only “upon an <u>updated showing</u> of the need for further delay.”</p> <p>... limits any <u>extensions to 90 days</u> or less, unless the facts of the case justify a longer delay.</p> <p>... adds <u>new public reporting</u> on the use of delayed notice warrants.</p>	<p>Not limited to terrorism. DOJ recently acknowledged that 88% of the search warrants issued under this section have been used in cases that have nothing to do with terrorism.</p> <p>Catch-all is too broad. Preserves catch-all for delays on the vague ground of seriously jeopardizing an investigation. Most of the 155 search warrants courts have approved have been based in part on the catch-all, jeopardy to an investigation, rather than a specific harm. A good prosecutor could fit almost any case into this clause.</p> <p>Still no time limit on delay. Before the Patriot Act, most circuit courts had <u>not</u> approved even reasonable but short delay in notice of physical searches. The conference report would not put any cap on the length of delay. Searches of American homes and businesses can still be kept secret for months or years under this Patriot Act power.</p> <p>Creates a month-long delay in notice as acceptable, subject to exceptions and an unlimited number of extensions. Defines “reasonable delay” as initially 30 days after a search warrant is executed, subject to exceptions. An unlimited number of extensions are allowed for periods of not more than 90 days each are allowed. No firm end-date of delay in notice required.</p>
---	--

<p>SECTION 206 OF THE PATRIOT ACT, AS AMENDED BY THE INTELL BILL, ALLOWS “JOHN DOE” ROVING WIRETAPS WHERE NEITHER THE IDENTITY NOR THE PHONE IS REQUIRED IN FOREIGN INTELLIGENCE INVESTIGATIONS.</p> <p>[Background: Since 1986, roving taps have been available in criminal investigations (including criminal terrorism investigations), subject to two safeguards – 1) that the “roving” tap identify the target, and 2) that agents “ascertain” the target is using the phone tapped. The Patriot Act created roving taps in intell investigations – approved by the FISA court--that don't require probable cause of crime. In 2005, the court approved 2073 orders for secret wiretaps or physical searches—there is no report on how many were roving.]</p> <p><i>Rhetoric:</i> The conference report ... requires a description of a “specific” target in both the application and the court order, if the target's true identity is unknown. ... requires “specific facts in the application” showing target's actions may thwart surveillance efforts. ... addresses concerns that “John Doe” roving wiretaps might be used to monitor someone described generically as an “Asian female” or “Hispanic male,” demanding information about a specific target. ...requires the FBI to <u>notify the court within 10 days</u> after beginning surveillance of any new phone... the notice must also include the “total number of electronic surveillances” conducted under the court's order. ...adopts <u>new reporting</u> to Congress, about use of “roving” authority.</p>	<p>Identity still not required. Permits roving wiretaps without identifying the target. Roving taps in intelligence investigations do not require agents to identify the target if his name is not known (only a “physical description” is required).</p> <p>Lacks needed ascertainment requirement. Not limited to circumstances where agents ascertain the target is using the telephone or facility. The lack of controls makes it more likely email and phone conversations of innocent people will be monitored, and that business, hotels or apartments could have many of phones tapped at once and for months at a time.</p> <p>Does not require “particularity” in the description of the target.</p> <p>Does require FBI to inform court of places tapped after-the-fact. If place is not known at the time the order is issued, requires applicant to notify issuing judge within 10 days, of the change of surveillance from the initial facility and reasons for change. This does not cure the fundamental problems with this extraordinary power.</p> <p>**MOST IMPORTANTLY—NOT EVEN FOLLOWED BY THE ADMINISTRATION, WHICH IS ENGAGING IN ILLEGAL WIRETAPPING OF AMERICANS WITHOUT A COURT ORDER. The Bush administration is treating these changes to the law as merely optional even though they are legal requirements. The administration is violating both the wiretapping and the pen register parts of FISA.</p>
---	---

DOJ's Patriot Act Talking Points	Patriot Act Reality
----------------------------------	---------------------

<p>SECTION 802 CREATES A DEFINITION OF DOMESTIC TERRORISM THAT ALLOWS FOR FORFEITURE OF AN ORGANIZATION'S ASSETS WITHOUT ADEQUATE NOTICE OF WHAT OFFENSES WOULD TRIGGER SUCH A PENALTY, INCLUDING MISDEMEANORS.</p> <p>[Background: Activities are “domestic terrorism” if they violate any state or federal criminal law, involve acts “dangerous to human life,” and “appear to be intended” to influence government policy or a civilian population “by intimidation or coercion.” Section 802 does not create a new crime, but can trigger enhanced seizure of assets, disclosure of educational and tax records as well as longer sentences and use of nationwide search warrants.</p> <p>Chills civil disobedience and risks assets. Domestic terrorism is defined so broadly that it could include acts of civil disobedience, such as protestors who block access to facilities or roads or trespass. Punishing civil disobedience is one thing but calling it terrorism and seizing assets is another and could chill citizens from protesting policies of any administration. Assets can be seized without criminal conviction and without a prior hearing.]</p> <p>Rhetoric: The conference report modifies the definition for asset forfeiture purposes.</p>	<p>Specifies which acts can trigger designation as domestic terrorism for asset forfeiture penalties. Changes the reference in the forfeiture statute from domestic terrorism to the federal crime of terrorism definition.</p> <p>Adds new specific offenses for trigger. Adds offenses to the federal definition of criminal terrorism to include receiving military-type training from a foreign terrorist organization and offenses relating to nuclear and weapons of mass destruction threats.</p> <p>No fix to Patriot Act's Title III money laundering expansion. Although the definition of domestic terrorism was changed with regard to forfeiture, other provisions of the Patriot Act, such as the expansions to the reach of money laundering laws allowing the Treasury Department to regulate an expansive group of private businesses—such as jewelers, hotel-casinos, pawn brokers and other companies—remains overly broad and intrusive.</p>
---	---