

Talking Points for PATRIOT Act Lobby Day, February 3, 2010

Why Congress should insist upon amendments to PATRIOT Act authorities before considering reauthorization

Amendments are necessary to protect the privacy of law-abiding Americans. The powers granted under the PATRIOT Act and other post-9/11 surveillance authorities have never received sufficient oversight despite recurring abuses. Where such powers are targeted to address potential terrorism, they are appropriate.

However, multiple government reports have documented widespread and systemic abuses requiring Congress to impose checks and balances. The looser the nexus between government powers and suspected terrorist activity, the more likely that the privacy of innocent Americans will be violated—and the less likely that there will be any national security benefit.

Some authorities under the PATRIOT Act (e.g., the lone wolf provision) are so poorly targeted they have been used only a handful of times, if ever. Others (e.g., national security letters) have been repeatedly and systematically abused, as confirmed by independent government analysis. And others (e.g., sneak and peek) reflect a bait and switch, with powers justified in the national security context being used nearly exclusively in routine drug war cases. The lack of transparency pervading the domestic surveillance arena continues, precluding Congress' ability to meet its constitutional mandate to check and balance the executive branch.

Finally, the PATRIOT Act's expiring provisions are the tip of an iceberg of constitutional offenses. While imposing long overdue reforms to the PATRIOT Act to ensure transparency and compliance with the law, Congress should also adopt reforms to rectify abuses of other laws, such as the Foreign Intelligence Service Act that Congress recently amended after then-Senator Obama pledged to introduce needed reforms.

Accordingly, measures to reauthorize the PATRIOT Act provisions due to expire at the end of February should be rejected, unless the final bill:

Provides greater protections for national security letters

National security letters (NSLs) are letters the government provides to telephone companies, banks, credit agencies, and similar institutions (the "recipients") to obtain certain communications, financial, and credit records about individuals without a court order. While authority for national security letters does not expire this year, the Department of Justice Inspector General has found substantial NSL abuses, and a federal appeals court has ruled that the gag order provisions of the national security letter statute violate the First Amendment, demonstrating a clear need for reform.

- Raise the standard for issuance. Records sought must pertain to a person tied to the agent of a foreign power and information sought must be relevant to a national security investigation. A mere certification by investigators does not suffice to meet this standard. Rather, a NSL should issue only upon the articulation of specific facts supporting a national security nexus.
- Limit the type of information that can be obtained by NSLs. Current statutes permit the use of NSLs to obtain basic subscriber information such as name, address, and billing information, as well as transactional records held by the recipient, such as to-and-from calling information. Transactional records are much more sensitive than basic subscriber information, however, and should be available only with a Section 215 court order or with criminal process.
- Restore First Amendment freedoms for recipients of gag orders. Limit the situations where non-disclosure ("gag") orders can be imposed on recipients, by requiring the government to justify a gag order to a court

and permit the court to evaluate the facts of each case independently. Also, courts should be allowed to disclose information to a recipient challenging a gag order under the rules in the Classified Information Procedures Act, a decades-old law that has been proven effective in protecting both classified information and the rights of litigants. This provision would not extend to sharing information with the actual subject of the records.

- Require mandatory minimization of information obtained by NSLs. Direct the Attorney General to issue guidelines that would govern the acquisition, retention, and dissemination of NSL information, so that information obtained about Americans is subject to enhanced protections and information obtained in error is not retained. Similar guidelines are required under the Foreign Intelligence Surveillance Act and have not proven burdensome.
- Limit the use of emergency NSLs to situations where there is a reasonable belief that danger is imminent.

Provides greater protections on Section 215 court orders

Section 215 of the PATRIOT Act gave authorities the power to obtain court orders for seizing records and other “tangible things” allegedly related to national security investigations. Investigators can obtain a Section 215 order by simply alleging relevance to a national security investigation. However, the justification for such an order can be based partly on activities protected by the First Amendment, such as reading prohibited or suspicious books. Moreover, the Justice Department’s own Inspector General has documented repeated abuse of investigative authorities, including privacy violations affecting hundreds of thousands, if not millions, of Americans.

- Require investigators to articulate specific facts supporting the relevance of records sought through a Section 215 order to a national security investigation.

Provides greater protections for charities

The material support statute criminalizes giving anything of value to a designated terrorist organization. However, it is broad enough to criminalize charitable activities such as giving food and water to civilians in war torn countries where working with designated groups is the only practical way for organizations to reach noncombatants.

- Protect innocent charitable giving from criminal prosecution. Impose an intent requirement (as with other criminal laws) so that individuals can be prosecuted only if they intend their donations to further the donee’s terror-related activities.

Provides greater protections on wiretaps

The “John Doe wiretap” provision of FISA allows the government to wiretap communications devices used by targets even if their precise identities are not known. The “roving wiretap” provision allows the government to wiretap any communications device that could be used by the target, including public telephones, library computer terminals, or other devices used by multiple individuals. Taken together, these provisions permit the FISA court to issue surveillance orders that specify neither the person nor the device to be wiretapped.

- Require the government to name either the person or device being targeted.

Provides protections against bulk collection of telecommunications

- Impose a ban on bulk collection conducted under the Foreign Intelligence Surveillance Act (FISA) Amendments Act. Ensure that foreign intelligence surveillance conducted under that law be limited to collecting international communications of foreign intelligence interest and not conducted in a dragnet fashion that could sweep in communications of literally millions of innocent Americans.

Why Congress should (a) support the End Racial Profiling Act and (b) oppose any exemption for national security

As demonstrated by “the underwear bomber” thwarted in December 2009, racial profiling is inadequate to meet our security needs. Demographic profiles lacking behavioral elements will always overlook potential threats.

Our country’s constitutional commitment to equal justice before the law precludes guilt by association, or suspicion on the basis of race, religion, or national origin. Security measures that cast suspicion along such lines, like the recent TSA screening guidelines, are counter-productive because they reinforce the narrative promoted by violent extremists: namely, that America is engaged in a war against Islam.

Communities of interest to law enforcement will be more likely to volunteer potentially useful information if they trust authorities. Profiling and other measures that marginalize specific communities (e.g., undercover infiltration of religious institutions and activist groups) undermine this trust—and by encouraging alienation instead, are ultimately counterproductive.