

**Setting the Record Straight:
An Analysis of the Justice Department's PATRIOT Act Website**
October 27, 2003

The Department of Justice has launched a website, www.lifeandliberty.gov, to defend the PATRIOT Act. As more and more people are raising concerns about the broad powers granted to the Justice Department – powers it does not need and is not using to fight terrorism – the Department is spending time and money on a public relations campaign, including a website and a tour of the country by the Attorney General to talk to law enforcement officers. But just as Attorney General Ashcroft has done in his speeches around the country, the website fails to engage on the substantive criticisms of the PATRIOT Act, instead touting provisions that no one objected to at the time the legislation was enacted and that no one has been objecting to since. Where the website does address controversial aspects of the law, it provides misleading, incomplete and, in some cases, incorrect information. Following is CDT's analysis of the claims made on that website.

DOJ CLAIM: "Congress enacted the Patriot Act by overwhelming, bipartisan margins."

- Congress voted overwhelmingly to pass the PATRIOT Act in October 2001. But Congress acted under intense time pressure and without serious debate and deliberation. The PATRIOT Act was signed into law a mere 5 weeks after the Administration's draft was first circulated – lightning speed for legislation. And on the House side, the version approved by the Judiciary Committee with some changes prompted by civil liberties concerns was replaced by a different version in the middle of the night, and a vote was taken just hours later – leaving members and their staff with literally not enough time to read what was in the lengthy bill. Any legislation adopted under these circumstances is likely to contain provisions that deserve to be revisited and corrected if appropriate.

DOJ CLAIM: The PATRIOT Act merely extended to terrorism cases authorities already provided in organized crime and drug trafficking cases, yet unavailable in terrorism cases. DOJ quotes Senator Biden as stating that "the FBI could get a wiretap to investigate the mafia, but they could not get one to investigate terrorists."

- That simply isn't true. The Justice Department had the ability to use wiretaps, including roving taps, in criminal investigations of terrorism, just as in other criminal investigations, long before the PATRIOT Act. Then what are they talking about? A special wiretap technique, the roving tap, was available in criminal investigations of

terrorists and drug dealers but was not available under the government's separate authority to investigate terrorism as a foreign counterintelligence matter under the Foreign Intelligence Surveillance Act (FISA). No civil liberties groups objected to adding roving tap authority to FISA. We did object to the fact that an important procedural safeguard applicable to roving taps in criminal cases was not applied to roving taps in intelligence cases. (See further discussion below.)

DOJ CLAIM: The PATRIOT Act “allows law enforcement to use surveillance against more crimes of terror.”

- As with many of the provisions touted on the DOJ website, this was not a controversial or contested provision of the PATRIOT Act. Section 201 of the PATRIOT Act added a list of seven new predicate offenses that could trigger a criminal wiretap order – with no objections from the civil liberties community. Furthermore, even prior to the PATRIOT Act, the FBI could have gotten an order under FISA to wiretap any suspected member of an international terrorist group.

DOJ CLAIM: The PATRIOT Act “allows federal agents to follow sophisticated terrorists trained to evade detection” with roving wiretap authority.

- As noted above, the FBI already had roving tap authority in criminal investigations of terrorism. The FBI did not have roving tap authority in intelligence investigations under FISA, but civil libertarians did not object to the PATRIOT Act's adding “roving” tap authority to FISA. The only dispute was about the standard that the FBI should be required to meet to use this authority – and in the end, the PATRIOT Act made it easier for the FBI to use roving taps under FISA than under the criminal procedures. First, under the PATRIOT Act the FBI does not have to ascertain that the target of the roving FISA wiretap is using the phone being tapped – an omission that could lead to innocent users having their conversations monitored. Second, the combined effect of the PATRIOT Act and the intelligence authorization bill that passed a few months later is that the FBI can now get a warrant to wiretap a phone or computer without specifying either the suspect under surveillance or the phones or computers to be tapped.

DOJ CLAIM: The PATRIOT Act “allows law enforcement to conduct investigations without tipping off terrorists” by delaying notification that their homes or offices have been searched.

- The FBI already had authority under FISA to conduct secret searches in international terrorism investigations. The PATRIOT Act permits the FBI to conduct so-called “sneak and peek” searches – where the FBI can search someone's home or office without notifying them until weeks or even months later – in criminal cases, including cases having nothing to do with terrorism. While courts had previously held that this delay in notification is permissible in limited circumstances, the PATRIOT Act provided statutory authority with entirely inadequate standards. The PATRIOT Act allows these extraordinary searches to be used in all criminal cases, not just terrorism cases, and the standard is so loose that it could arguably be used in almost every criminal case. The presumption has long been that law enforcement officers have to knock and announce themselves when they execute a search warrant, and an exception to that rule should be made only in limited circumstances with strict guidelines – which the PATRIOT Act does not contain.

DOJ CLAIM: The PATRIOT Act “allows federal agents to ask a court for an order to obtain business records in national security cases.”

- The FISA court order for business records has no meaningful standard. Section 215 of the PATRIOT Act permits the FBI to obtain a wide range of business records – including library, bookstore, medical, travel and other records – in any intelligence investigation, under a legal standard so low that it essentially results in a judicial rubber stamp. The FBI doesn’t even have to name the person whose records it is seeking, but rather can sweep up entire databases indiscriminately. Given the vast array of records available to the FBI under this section, it should be subject to tougher standards. The FBI should have to name an individual whose records it is seeking and offer some factual basis for believing that the person is a spy or linked to terrorism in some way.

DOJ CLAIM: “The PATRIOT Act facilitated information sharing and cooperation among government agencies so that they can better ‘connect the dots.’”

- The outcry over the PATRIOT Act has little to do with the increased ability of federal agencies to share relevant intelligence or increase their coordination. In fact, there was never a legal bar to intelligence agencies sharing information with prosecutors. Intelligence and law enforcement officials weren’t effectively sharing information and using their existing powers *not* because of legal barriers, but because of their overly strict interpretation of then-existing law, cultural problems, and turf wars among agencies.

DOJ CLAIM: The PATRIOT Act “allows law enforcement officials to obtain a search warrant anywhere a terrorist-related activity occurred.”

- It is certainly harder for an individual to challenge a warrant if the issuing court is thousands of miles away, but the proposal to authorize multi-jurisdiction search warrants was not a significant concern at the time the PATRIOT Act was passed, and has not been a major focus of the concerns raised about the PATRIOT Act in recent months.

DOJ CLAIM: The PATRIOT Act “allows victims of computer hacking to request law enforcement assistance in monitoring the ‘trespassers’ on their computers” and places “electronic trespassers on the same footing as physical trespassers.”

- Section 217 of the PATRIOT Act allows Internet Service Providers, universities and network administrators to authorize government surveillance of “computer trespassers” without a judicial order, without notice to the person being monitored, without reporting to a judge after the fact, without a suppression remedy, without congressional reporting, and without a liability remedy for the person being monitored. That is a far cry from burglary victims being able “to invite [police] officers into their homes to catch burglars,” as DOJ argues. Under those circumstances, the burglar is well aware that the victim thinks the burglar is trespassing and that the police are investigating – and has the full panoply of protections available in the criminal system. Anyone designated a “computer trespasser” has no such rights or knowledge.

DOJ CLAIM: “The PATRIOT Act increased the penalties for those who commit terrorist crimes.”

- Yet again, the Justice Department is defending a section of the PATRIOT Act that has not been challenged. The civil liberties community has not objected to the increased criminal penalties in the PATRIOT Act.

The following claims appear at http://www.lifeandliberty.gov/subs/u_myths.htm.

DOJ CLAIM: “Peaceful political organizations engaging in political advocacy” cannot be considered terrorists under the PATRIOT Act’s new definition of “domestic terrorism.”

- Under the PATRIOT Act, a violation of some criminal law involving risk of serious injury must occur before a person can be labeled a domestic terrorist. But it is easy to see how if an anti-abortion activist blocks traffic as part of a protest, or swings a sign and hits someone on the head, he could be labeled a terrorist. Such activities should be illegal, but they should not be subject to the threat of being labeled “terrorism,” triggering application of draconian law enforcement powers, such as the power to seize property – including cars, boats and homes.

DOJ CLAIM: “The PATRIOT Act specifically protects Americans’ First Amendment rights.”

- Section 215 provides that an investigation in which business records are sought shall “not be conducted of a United States person [U.S. citizen or green card holder] solely upon the basis of activities protected by the first amendment.” That caveat has little practical effect because few if any investigations would be conducted *solely* based on First Amendment activities. Indeed, the caveat makes it clear that information about First Amendment activities can be collected.

DOJ CLAIM: In defending sneak and peek searches, DOJ states that the Supreme Court has already concluded that delayed notification is constitutionally permissible.

- Contrary to the Justice Department’s assertion, the Supreme Court has never ruled that delayed notification is permissible for execution of a warrant to physically search someone’s home or office. The case cited by the Justice Department, *Dalia v. United States*, 441 U.S. 238 (1979), held that a covert entry was permitted to install a bug because there was no other way to effectively execute the order authorizing the bug. In the context of wiretaps and bugs, it would nonsensical to notify someone that you are planning to monitor their communications. That rationale simply does not apply in the context of physical searches. The Supreme Court has never ruled on the constitutionality of sneak and peek searches.

For more information: Jim Dempsey, (202) 637-9800 ext. 112, jdempsey@cdt.org
Lara Flint, (202) 637-9800 ext. 113, lflint@cdt.org