

MEMORANDUM

TO: All Interested Parties

FROM: John W. Whitehead, President

DATE: August 27, 2003

RE: Life, Liberty and the Pursuit of Terrorists: A Rutherford Institute Response to Attorney General John Ashcroft's "Patriot Act Tour" and Website

In conjunction with his nationwide tour to defend the U.S.A. PATRIOT Act, Attorney General John Ashcroft recently launched a new Internet website, www.lifeandliberty.gov. The website, draped in an American flag and entitled "Preserving Life and Liberty," offers Ashcroft's "talking points" in defense of the Act in a media-friendly format.

The site opens with the bold statement that the Patriot Act has been instrumental in foiling new terrorist attacks after 9/11:

Since its passage following the September 11, 2001 attacks, the Patriot Act has played a key part - and often the leading role - in a number of successful operations to protect innocent Americans from the deadly plans of terrorists dedicated to destroying America and our way of life.

This success, says the Justice Department, has come at no real price to fundamental American freedoms protected by the Bill of Rights, for "in passing the Patriot Act, Congress provided for only modest, incremental changes in the law. Congress simply took existing legal principles and retrofitted them to preserve the lives and liberty of the American people from the challenges posed by a global terrorist network."

But does the Justice Department's glowing review of the Patriot Act's track record stand up to close scrutiny? In the interest of providing an objective check to an issue charged with patriotic emotion, The Rutherford Institute offers the following point-for-point response to Attorney General Ashcroft:

- I. Does the Patriot Act Merely Permit Investigators to Use Tools Already Available to Combat Organized Crime and Drug Trafficking?
 - A. Expanding the Scope of the Wiretap Act.

The Life and Liberty website charges that "Many of the tools the Act provides to law enforcement to fight anti-terrorism [sic] have been used for decades to fight organized crime and drug dealers, and have been reviewed and approved by the courts." The Justice Department

quotes Sen. Joe Biden, who exclaimed during the floor debate on the Act that “the FBI could get a wiretap to investigate the Mafia, but they could not get one to investigate terrorists.”

The Justice Department’s statements in this regard are misleading. While it is true that wiretaps have been available for many years to combat serious crimes such as racketeering and Mafia-related drug smuggling and violence, wiretap warrants have always been available to investigate federal crimes committed by terrorists. The Patriot Act did not change the rules governing statutory wiretap orders. Instead, it expanded the scope of availability for wiretap warrants without clearly defining what crimes could be investigated via wiretapping.

The Wiretap Act of 1968, 18 U.S.C. § 2510 *et seq.*, was enacted by Congress in order to curb abuses by law enforcement in the electronic monitoring of ordinary citizens.¹ The Wiretap Act ordinarily requires a court order based upon an affidavit establishing probable cause to believe a crime has been or is about to be committed and that the search will reveal evidence thereof. 18 U.S.C. §§ 2516, 2518. In this respect, the Wiretap Act simply mirrors the fundamental protections for privacy afforded by the Fourth Amendment since the United States Supreme Court has declared that the Fourth Amendment itself “does not permit the use of warrantless wiretaps [even] in cases involving domestic threats to national security.”²

In spite of this high standard, however, wiretap orders are virtually never denied. For the years 1996 through 2000, reported wiretap requests by federal and state agencies totaled 6,205; only three were denied, an approval rate of *99.9%-plus*.³ Thus, in practical effect, the Wiretap Act has never presented a real hurdle to Justice Department attempts to electronically monitor alleged perpetrators. Despite this apparent lack of judicial checks on the availability of wiretap orders, the Patriot Act expanded their availability even further. Sections 201 and 202 of the Patriot Act amend the Wiretap Act to allow the FBI to obtain wiretap warrants for “terrorism” investigations, “chemical weapons” investigations, or “computer fraud and abuse” investigations. This expands the federal government’s wiretap authority into the broad areas allegedly related to “terrorism” and computer abuse investigations without providing a definition of these types of crimes to serve as a check on this greatly expanded authority to monitor citizens.

Moreover, contrary to the Attorney General’s assertion, federal law had *already* protected computer service providers from hacking or fraud.⁴

B. “Roving Wiretaps” Provided by Rubber Stamp.

The Justice Department is also misleading the public by claiming that the Patriot Act’s grant of new “roving wiretap” powers only broadens existing law enforcement authority to “terrorism” investigations. The roving wiretaps that have been used “for years,” according to the Life and Liberty website, to investigate racketeering and drug trafficking have been obtained under the nominal safeguards of the Wiretap Act, which, as stated above, requires probable cause. The roving wiretap powers granted by Sections 206 and 207 of the Patriot Act are provided through the Foreign Intelligence Surveillance Act (FISA) Court, a secret federal court that authorizes warrants on less than probable cause and operates as a virtual rubberstamp for law enforcement authorities, having denied only one request for a warrant in its 25-year existence.

Furthermore, this provision of the Act also eliminated two extremely important checks from the system that have historically provided a measure of accountability for the validity of a warrant. First, the amendment allowed the issuance of so-called “blank warrants,” by which the parties required to respond to the order need not be listed on the face of the document. This places subjects of a warrant such as computer communications providers in the position of having to accept the validity of the warrant and its application to them virtually without specificity or question. Second, if the order were issued by a far-flung court, as will usually be the case, the hindrances of geography and expense ordinarily would be prohibitive for a party that desires to challenge the validity of such an order in court.

C. Secret Searches Routinely Available.

The Justice Department also employs the same misleading rhetoric by asserting that the Patriot Act’s provisions allowing so-called “sneak and peak” and “black bag” searches, in which businesses, residences or computers are searched (“sneak and peak” warrants) and in some cases seized (“black bag” warrants), only authorize types of searches that “federal courts in narrow circumstances long have allowed.” Once again, although on occasion federal judges have issued warrants for such searches based on probable cause, the Fourth Amendment and the federal statutes governing physical searches of premises have never made such searches routinely available. Notice of the execution of a warrant has long been held to be an important component of the “reasonableness” of a search under the Fourth Amendment.⁵ In fact, this ancient common law right predates our Bill of Rights. As the Supreme Court has noted, this standard dates back to the Magna Carta era.⁶ In view of the established nature of the notice requirement, the Supreme Court has held that a search or seizure of a dwelling may be constitutionally defective if police officers entered without prior announcement.⁷ The kind of “notice” referred to by the Justice Department is not notice at all, since the owner has no way of knowing whether his house and belongings were pilfered or rifled through by law enforcement officers or burglars until a polite letter arrives giving him “notice” of the warrant.

Because this right is so central to personal autonomy and privacy as against the State, the notice requirement is codified in the federal criminal procedure statutes.⁸ These statutes allow the subject of the warrant an opportunity to respond by challenging the lawful authority of the warrant or to prevent its defective execution, such as when the wrong address is targeted or the subject no longer resides at the address.⁹ A legion of tragic incidents resulting from execution of “no-knock” warrants demonstrates the potential dangers inherent in serving such warrants on innocent victims.¹⁰

D. Business Records Seized and Business Owners Gagged.

The website also lauds the Patriot Act provision that allows court orders for business records in terrorism investigations. Reasoning that grand juries have always had the power to subpoena business records, it cites one case where a grand jury subpoena of library records was employed to search for a killer inspired by an obscure Scottish poet. Grand jury inquiries, however, are focused on specific crimes and specific targets; the FISA court, which issues

business records subpoenas under the Patriot Act, gives federal authorities virtual *carte blanche* subpoena powers based on less than probable cause. Notably, the Act also gags business owners from publicly challenging such subpoenas: “No person shall disclose to any other person...that the Federal Bureau of Investigation has sought or obtained tangible things under this section.” In other words, the business is gagged from disclosing that it has been the subject of an FBI search and seizure, including presumably to the media.

Ashcroft is also being duplicitous in urging that sufficient safeguards are available for business owners. Ashcroft defends the Act’s business records seizure provision on the Life and Liberty website by arguing that the FISA court can order secret production of business records such as bookstore and video store rental records “only after the government demonstrates the records concerned are sought for an authorized investigation.” But on the stump, speaking recently on *Fox News Sunday*, Ashcroft argued for an extension to the Patriot Act that would remove this key safeguard altogether and permit the Justice Department to issue its own orders for business records without court oversight.¹¹ Ashcroft regards this power, along with other similar powers the Bush Administration may ask of Congress, as just “some more tools in our tool kit against terror.”¹²

II. Does the Patriot Act “Facilitate Information Sharing and Cooperation Among Government Agencies So That They Can Better ‘Connect the Dots’”?

The Justice Department belittles legal barriers to information sharing between domestic law enforcement and intelligence officials that have been in place for decades, stating, “The government’s prevention efforts should not be restricted by boxes on an organizational chart.” What the Attorney General’s position amounts to, though, is that the federal law enforcement and intelligence “organizational chart” should be centralized under one person, namely the Attorney General. Section 808 of the Act reassigns the authority for investigating numerous federal crimes of violence from other federal law enforcement agencies such as the Secret Service, the Bureau of Alcohol, Tobacco and Firearms (under the Treasury Department) and the Coast Guard to the Attorney General, in addition to his authority for investigating “all federal crimes of terrorism.”¹³ These new areas of investigation include assault against specified federal high office holders;¹⁴ threats of homicide, assault, intimidation, property damage, arson or bombing;¹⁵ arson or bombing of federal property;¹⁶ conspiracy to destroy property of a foreign government;¹⁷ malicious mischief against United States government property;¹⁸ destruction of property of an energy utility;¹⁹ assault against presidential or White House officials;²⁰ sabotage of harbor defenses;²¹ and sabotage of war industry facilities.²² Essentially for the sake of combating terrorism, Congress has granted the Attorney General the power to investigate not only acts of terrorism but most acts of violence against public officers and property. The extent to which these executive branch powers have been consolidated in one official, i.e., the Attorney General, is unprecedented in recent history.²³

At the same time that the Bush Administration has centralized authority for international and domestic law enforcement in the Justice Department, the Administration, through the Patriot Act, has also transferred authority for coordinating *domestic* intelligence gathering from the Justice Department to the Central Intelligence Agency. The Patriot Act added a new subsection (c)(6) to the statute defining the CIA Director’s authority to provide that the CIA Director shall:

(6) establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, *et seq.*) and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes.²⁴

This coordinating role was formerly taken by the Attorney General. Essentially, the Patriot Act has given the CIA the central role in gathering and using intelligence information garnered from *domestic* sources, including intelligence on United States citizens and residents. This authority raises an inherent conflict with another section of the statute ostensibly limiting the CIA's authority, § 403-3(d)(1), which provides that the CIA "shall have no police, subpoena, or law enforcement powers or internal security functions." By placing the CIA over the Justice Department and the FBI, this provision of the Patriot Act turns on its head existing policy and practice that was put in place as a result of CIA abuses during the Cold War era and permits the CIA to begin once again to spy on American citizens.²⁵ Moreover, as the Attorney General has repeatedly said, the federal government reserves the right to monitor religious groups and charitable organizations as well, a practice that has subjected federal law enforcement authorities to considerable judicial scrutiny for its chilling effect on the right to free association and worship under the First Amendment.²⁶ Also, the CIA has at the same time been given unprecedented access to a broad range of intelligence gathering powers that allow information collection and monitoring of American citizens under other provisions of the Patriot Act.²⁷

III. Does the Patriot Act Assure Americans That Only Dangerous "Terrorists" Will Be Targeted?

Although the Justice Department is ostensibly targeting a "narrow class of individuals" as suspected terrorists, it has greatly expanded that class of suspects through the Patriot Act. Section 802 of the Act amends Chapter 113B of the criminal code, 18 U.S.C. § 2331, to add a new definition of "domestic terrorism" to include activities that:

- (A) Involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
- (B) Appear to be intended –
 - (I) to intimidate or coerce a civilian population;
 - (II) to influence the policy of a government by mass destruction, assassination, or kidnapping; and
- (C) Occur primarily within the territorial jurisdiction of the United States.²⁸

Likewise, Section 808 amends 18 U.S.C. § 2332b to include any such acts that result in virtually any federal crime of violence.²⁹ Conceivably, these extensions of the definition of "terrorist"

could bring within their sweep diverse domestic political groups that have been accused of acts of intimidation or property damage such as Act Up, PETA, Operation Rescue, and the Vieques demonstrators, among others.

The Attorney General recently assured the Senate: “Since 1983, the United States government has defined terrorists as those who perpetrate premeditated, politically motivated violence against noncombatant targets.”³⁰ If that is true, it certainly begs the issue of why the Bush Administration felt the need to now redefine “terrorism” to include within the scope of the term a wide variety of domestic criminal acts of violence.

CONCLUSION

Attorney General Ashcroft charges that passage of the Patriot Act radically changed “a culture of law enforcement inhibition” in America.³¹ When the Act restricts or weakens constitutional and statutory protections for fundamental rights of privacy and personal autonomy, including a right characterized by the Supreme Court as being “as old as the Magna Carta,” one can surely forgive a reasonable observer for wondering whether, in throwing off “inhibitions” on law enforcement for the sake of its pursuit of terrorists, America has carefully calibrated the ramifications of this authoritarian revolution for its continued commitment to the life and liberty of all its people.

Footnotes

¹ See *Mitchell v. Forsyth*, 472 U.S. 511 (1985) (discussing at length history of federal wiretaps and adoption of the Wiretap Act).

In passing Title III, Congress found:

(a)... There has been extensive wiretapping carried on without legal sanctions and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings....

(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused.

Act June 19, 1968, P.L. 90-351, Title III, § 801, 82 Stat. 211. A 1986 amendment to the Act provided, “Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.” Act Oct. 21, 1986, P.L. 99-508, Title I, § 107, 100 Stat. 1858.

² *Mitchell v. Forsyth*, 472 U.S. at 514, citing *United States v. United States District Court*, 407 U.S. 297 (1972) (*Keith*). “*Keith* finally laid to rest the notion that warrantless wiretapping is permissible in cases involving domestic threats to national security.” *Mitchell*, at 534.

³ See Table, “Authorized Interceptions Granted Pursuant to 18 U.S.C. § 2519 as Reported in Wiretap Reports for Calendar Years 1990-2000,” www.uscourts.gov/wiretap00/table700.pdf.

⁴ See generally 18 U.S.C. § 2511(2)(a)(I) (2000) (permitting interception and disclosure of communications by a computer service provider to protect the provider’s rights or property, including in cases of fraud).

⁵ *Wilson v. Arkansas*, 514 U.S. 927 (1995) (common law knock-and-announce principle formed a part of the Fourth Amendment reasonableness inquiry); *Richards v. Wisconsin*, 520 U.S. 385 (1997) (there is no “felony drug search exception” to the knock and announce requirement).

⁶ *Wilson*, 514 U.S. at 932, n. 2.

⁷ *Wilson*, *supra*.

⁸ See 18 U.S.C. § 3109 (“The officer may break open any outer or inner door or window of a house, or any part of a house, or anything therein, to execute a search warrant, if, after notice of his authority and purpose, he is refused admittance....”).

⁹ *Wilson*, 514 U.S. at 931-933 (discussing historical reasons for rule). The Court in *Richards* subsequently elaborated:

While it is true that a no-knock entry is less intrusive than, for example, a warrantless search, the individual interests implicated by an unannounced, forcible entry should not be unduly minimized. As we observed in *Wilson v. Arkansas*, the common law recognized that individuals should have an opportunity to comply themselves with the law and to avoid the destruction of property occasioned by a forcible entry. These interests are not inconsequential.

Additionally, when police enter a residence without announcing their presence, the residents are not given any opportunity to prepare themselves for such an entry. The State pointed out at oral argument that, in *Wisconsin*, most search

warrants are executed during the late night and early morning hours. The brief interlude between announcement and entry with a warrant may be the opportunity that an individual has to pull on clothes or get out of bed.

520 U.S. at 393, n. 5 (citations omitted).

¹⁰ See, e.g., *Atkins v. City of Dallas*, 1997 U.S. Dist. LEXIS 4983 (N.D. Tex.) (officers executed “dynamic entry” with battering rams and flashbang devices, black uniforms and masks; suspect had vacated home one month earlier); “Officer Who Killed Grandfather in Mistaken Raid was Named in 2 Force Suits,” *Los Angeles Times*, October 5, 1999; T. Lynch, *Another Drug War Casualty*, Cato Institute, November 30, 1998 (detailing death of Pedro Oregon Navarro in raid on wrong address); “Cops Kill Man, Raid Wrong House,” *Associated Press*, October 6, 2000 (raid of home next door to correct address results in death of occupant); “Police Officer Pleads Guilty in ‘No-Knock’ Drug Raid Killing,” *Associated Press*, October 5, 2000; “Unity Plea in Slaying’s Wake,” October 5, 2000, *Modesto Bee* (11-year-old boy killed in SWAT raid); Office of the District Attorney, County of Ventura, “Report on the Death of Donald Scott,” March 30, 1993 (seizure and forfeiture operation targeting alleged marijuana growth on economically desirable property resulted in shooting death of 61-year-old owner; no marijuana was found). In Boston in 1994, a mistaken SWAT raid on a 75-year-old minister’s home resulted in the man’s death from a heart attack; police had targeted the wrong house. “Boston to Give Victim’s Widow \$1 Million in Wrongful Death Suit,” *New York Times*, April 25, 1996.

¹¹ Dan Eggen, “GOP Bill Would Add Anti-Terror Powers,” *Washington Post*, August 21, 2003, A03.

¹² *Id.*

¹³ P.L. 107-56, Title VIII, § 808, 115 Stat. 378.

¹⁴ This crime is codified at 18 U.S.C. § 351(e).

¹⁵ Codified at 18 U.S.C. § 844(e).

¹⁶ Codified at 18 U.S.C. § 844(f)(1).

¹⁷ Codified at 18 U.S.C. § 956(b).

¹⁸ Codified at 18 U.S.C. § 1361.

¹⁹ Codified at 18 U.S.C. §§ 1366(b) and (c).

²⁰ Codified at 18 U.S.C. § 1751(e).

21 Codified at 18 U.S.C. § 2152.

22 Codified at 18 U.S.C. § 2156.

23 The administration's centralization of authority and resistance to accountability bring to mind James Madison's words in FEDERALIST NO. 51. Addressing the inherent tension between liberty and authority in democratic governments, Madison said:

If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the difficulty lies in this: You must first enable the Government to control the governed; and in the next place, oblige it to control itself.

24 50 U.S.C. § 403-3(c)(6).

25 The most notorious, but certainly not the only, example of the CIA's abuse of this monitoring power is that of "Operation CHAOS," initiated in 1967 to monitor American citizens who protested against the Vietnam War. *See generally Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982); *In re Halkin*, 598 F.2d 176 (D.C. Cir. 1979); *Hrones v. Central Intelligence Agency*, 685 F.2d 13 (1st Cir. 1982); *National Lawyers' Guild v. Attorney General*, 96 F.R.D. 390 (S.D.N.Y. 1982); *Grove Press, Inc. v. CIA*, 483 F.Supp. 132 (S.D.N.Y. 1980); *Ferry v. CIA*, 485 F.Supp. 664 (S.D.N.Y. 1978); *Krause v. Rhodes*, 535 F.Supp. 338 (N.Dist. Ohio 1979); *Socialist Workers' Party v. Attorney General*, 642 F.Supp. 1357 (S.D.N.Y. 1986). CHAOS was concerned with the degree of influence exerted over critics of the Johnson Administration's Vietnam policy by "Soviets, Chicoms [Chinese Communists], Cubans and other Communist countries.... Of particular interest is any evidence of foreign direction, control, training or funding." *Halkin*, 690 F.2d at 982, n. 8. *See generally Report to the President by the Commission on CIA Activities Within the United States* (1975) (the "Rockefeller Report"); *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, Sen. Rep. No. 94-755, 94th Cong., 2nd Sess. (1976). Groups targeted included "radical students, anti-Vietnam war activists, draft resisters and deserters, black nationalists, anarchists, and assorted 'New Leftists.'" 690 F.2d at 982, n. 9. The CIA maintained several thousand computerized files on Americans involved in these activities. *Id.* at 982. Its activities ranged from infiltration and mail monitoring to inclusion of several dozen Americans on a "watchlist," which enabled the CIA to scan and intercept all telecommunications containing references to those names. 690 F.2d at 983-984.

26 "Ashcroft: Groups Could Be Monitored," *Washington Post*, December 3, 2001. *See, e.g., United States v. Aguilar*, 883 F.2d 662 (9th Cir. 1989) (describing infiltration and extensive monitoring of churches by INS officials investigating alleged alien smuggling); *Mockaitis v. Harclerod*, 104 F.3d 1522 (9th Cir. 1997) (Fourth Amendment rights of clergy and prisoner

were violated by surreptitious taping of prison confessional).

27 For a description of how this inter-agency information gathering works, see “Personnel from Assorted Agencies Work Together at FBI Headquarters,” *Washington Post*, October 14, 2001, A16 (describing agents of FBI, CIA, NSA, DIA, Customs and others working side-by-side in anti-terrorism headquarters of the FBI and CIA). The Attorney General’s rationale for this expanded information gathering and sharing capability is similar in tone, if not intent, to the Vietnam-era CIA’s rationale for citizen monitoring:

[L]aw enforcement needs a strengthened and streamlined ability for our intelligence gathering agencies to gather the information necessary to disrupt, weaken and eliminate the infrastructure of terrorist organizations. Critically, we also need the authority for law enforcement to share vital information with our national security agencies in order to prevent future terrorist attacks.

Testimony of Attorney General Ashcroft, September 25, 2001.

28 P.L. 107-56, Title VIII, § 802.

29 P.L. 107-56, Title VIII, § 808. The Act’s amendment to 18 U.S.C. § 3077, which includes “domestic terrorism” within the rewards program provided by the Justice Department for information relating to terrorist acts, further confirms that the Justice Department will routinely employ this broader definition of “terrorism.” See P.L. 107-56, Title VIII, § 802(b).

30 Testimony of Attorney General Ashcroft, December 6, 2001. The Attorney General is apparently referring to the former versions of the provisions cited above, which now employ broadly expanded definitions of “terrorism” pursuant to the Patriot Act amendments.

31 Remarks to American Enterprise Institute, August 19, 2003, available at www.lifeandliberty.gov.