Legal Memorandum
Published by The Heritage Foundation
No. 10
April 30, 2004

The SAFE Act Will Not Make Us Safer

Edwin Meese III and Paul Rosenzweig

The USA PATRIOT Act,[1] a law passed with overwhelming support in Congress immediately following the September 11 terrorist attacks, has been the subject of many recent attacks and criticisms.[2] Opponents argue that various provisions of the Patriot Act, and related laws and practices, have greatly infringed upon American liberties while failing to deal effectively with the threat of terrorism.

Criticism of the anti-terrorist campaign is not limited to the Patriot Act; many other aspects of the Bush Administration's domestic response to terrorism have come under fire. To some degree, the Patriot Act as conceived by the public is broader than its actual provisions. Its very name has come to serve as a symbol for all of the domestic anti-terrorist law enforcement actions. It has become a convenient shorthand formulation for all questions that have arisen since September 11 about the alleged conflict between civil liberty and national security.

But the Patriot Act is a real law, with real purposes and real provisions. Too much of the debate has focused on the Act not as it truly is but as people perceive it to be. Most of the proposals for reform mistake the appearance of potential problems and abuse (the myth) with the reality of no abuse at all[3]—and, thus, the case for change has not been made.

The Security and Freedom Ensured Act of 2003 (the "SAFE Act")[4] is emblematic of this trend. It purports to be based upon an assessment of the necessity for change, yet its major substantive provisions lack any factual basis for con-

Talking Points

- We cannot decide policy based upon an over-wrought sense of fear. Most of the steps proposed to combat terrorism were previously used to combat organized crime, and there is no evidence of any real abuse. No First Amendment liberties have been curtailed, no dissent or criticism suppressed.
- In reviewing our policies and planning for the future, we must be guided by the realization that this is not a zero-sum game. We can achieve both goals—liberty and security—to an appreciable degree.
- The key is empowering government to do the right things while exercising oversight to prevent the abuse of authority. So long as we keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on our fundamental liberties can be avoided.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/lm10.cfm

Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Ave., NE
Washington, DC 20002–4999
(202) 546-4400 heritage.org

cluding that changes are necessary. Often the proposals rest on incomplete legal analysis and would make America's response to terrorism less effective. In the end, they appear to be little more than a political fig leaf, intended to allow politicians to assert that they have responded to the public will and "fixed" the Patriot Act.

But capitulating to hysteria is pandering, not leadership. The SAFE Act will not make America safer.

This paper addresses the three principal substantive provisions of the SAFE Act: Section 2, which would limit the use of roving wiretaps; Section 3, which would modify traditional authority to delay notification of a search; and Sections 4 and 5, which would limit the ability of law enforcement and intelligence authorities to secure business records relating to terrorist activity. Each of these proposed revisions is ill-conceived and ought, on the merits, to be rejected.[5]

Roving Wiretaps: a Useful Tool

Section 206 of the Patriot Act authorized the use of "roving wiretaps"—that is, wiretaps that follow an individual and are not tied to a specific telephone or location—in terrorism investigations. America's original electronic surveillance laws (the Foreign Intelligence Surveillance Act ("FISA") of 1978 and Title III of the Omnibus Crime Control Act of 1968)[6] stem from a time when phones were the only means of electronic communications and all phones were connected by hard wires to a single network.

Roving wiretaps have arisen over the past 20 years for use in the investigation of ordinary crimes (e.g., drug transactions or organized crime activities) because modern technologies (cell phones, BlackBerries, and Internet telephony) allow those seeking to evade detection the ability to change communications devices and locations at will. Section 2 of the SAFE Act would unwisely restrict the use of roving wiretaps in terrorism investigations.

Getting a FISA Warrant to Conduct Electronic Surveillance

To begin with, one must understand the general structure of laws governing when law enforcement or intelligence agents may secure authorization to conduct electronic surveillance relating to suspected foreign intelligence or terrorism activity. Title III (the statute governing electronic surveillance for domestic crime) allows a court to enter an order authorizing electronic surveillance if "there is probable cause for belief that an individ-

1. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107–56, 115 Stat. 272 (Oct. 26, 2001).
2. Typical of the public criticism was the recent resolution of the National League of Cites calling for repeal of various portions of the Patriot Act. *See* Audrey Hudson, "Cities in Revolt over Patriot Act," *Washington Times*, Jan. 5, 2004. A number of cities and municipalities have passed similar resolutions. *See, e.g.*, Jessica Garrison, "L.A. Takes Stand Against Patriot Act," L.A. Times at B4 (Jan. 22, 2004). Responding to these criticisms, President Bush has called for reauthorization of the Patriot Act. *See* State of the Union (Jan. 20, 2004) ("The terrorist threat will not expire on [a] schedule. Our law enforcement needs [the Patriot Act] to protect our citizens.").
3. The Inspector General for the Department of Justice has reported that there have been no instances in which the Patriot Act has been invoked to infringe on civil rights or civil liberties. *See* Report to Congress on Implementation of Section 1001 of the USA Patriot Act (Jan. 27, 2004); *see also* "Report Finds No Abuses of Patriot Act," *Washington Post* at A2 (Jan. 28, 2004). This is consistent with the conclusions of others. For example, at a Senate Judiciary Committee Hearing on the Patriot Act, Senator Joseph Biden (D–DE) said that "some measure of the criticism [of the Patriot Act] is both misinformed and overblown." His colleague, Senator Dianne Feinstein (D–CA) said: "I have never had a single abuse of the Patriot Act reported to me. My staff…asked [the ACLU] for instances of actual abuses. They…said they had none." Even the lone Senator to vote against the Patriot Act, Russ Feingold (D–WI), said that he "supported 90 percent of the Patriot Act" and that there is "too much confusion and misinformation" about the Act. *See* Senate Jud. Comm. Hrg. 108th Cong, 1st Sess. (Oct. 21, 2003). These views—from Senators outside the Administration and an internal watchdog—are at odds with the fears often expressed by the public.
4. *See* S. 1709 (108th Cong.). The SAFE Act is co-sponsored by Senators Craig (R–ID), Durbin (D–IL), Crapo (R–ID), Feingold (D–WI), Sununu (R–NH), Wyden (D–OR), and Bingaman (D–NM).
5. A more extensive version of portions of this paper will appear in Paul Rosenzweig, "Civil Liberty and the Response to Terrorism," 42 Duq. L. Rev. ___ (2004) (forthcoming). Material from the article is reprinted here with permission.
6. The FISA governs applications for electronic surveillance in matters relating to foreign intelligence, espionage, counterintelligence, and terrorism. Title III governs applications for electronic surveillance involving the investigation of domestic crimes.

ual is committing, has committed or is about to commit" one of a list of several specified crimes.[7]

FISA (the statute governing intelligence and terrorism surveillance) has a parallel requirement: A warrant may issue if there is probable cause to believe that the target of the surveillance is a foreign power or the agent of a foreign power.[8] FISA also requires that the government establish probable cause to believe that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used" by the foreign power or the agent of the foreign power who is the target of surveillance.[9] FISA court warrants thus are issued by federal judges, upon a showing of probable cause, and describe the things to be seized with particularity—the traditional three-prong test for compliance with the warrant clause requirements of the Fourth Amendment.[10]

Thus, no one can argue that these FISA warrants violate the Constitution. To the contrary, as the Foreign Intelligence Surveillance Court of Review recently made clear, the FISA warrant structure is "a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens."[11] This is so because, as the court recognized, there is a difference in the nature of "ordinary" criminal prosecution and that directed at foreign intelligence or terrorism crimes:

> The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity.[12]

Roving Wiretaps and Section 206

Roving wiretaps (whether used in foreign intelligence or domestic criminal investigations) are, as noted, a response to changing technologies. Phones are no longer fixed in one place and can move across state borders at the speed of flight. Sophisticated terrorists and criminals can change phones and communications devices constantly in an attempt to thwart interception.

In response to these changes in technology, in 1986 Congress authorized a relaxation of the particularity requirement for the investigation of drug offenses.[13] Under the modified law, the authority to intercept an individual's electronic communication was tied only to the individual who was the suspect of criminal activity (and who was attempting to

7. *See* 18 U.S.C. §2518(3)(a). Thus, Title III wiretaps are not available at all for the investigation of many relatively trivial criminal offenses.
8. *See* 50 U.S.C. §1805(a)(3)(A). A "foreign power" includes both foreign governments and groups engaged in international terrorism. *See* 50 U.S.C. §1801(a)(1). The definition of an agent of a foreign power includes any person who "knowingly engages in clandestine intelligence gathering activities…which…involve or may involve a violation of the criminal statutes of the United States" or "knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof." 50 U.S.C. §§1801(b)(2)(A), (C). International terrorism is, in turn, defined as "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States…or that would be a criminal violation if committed within the jurisdiction of the United States." 50 U.S.C. §1801(c)(1). Thus, one of the great and enduring myths about FISA and the Patriot Act is that they allow electronic surveillance willy-nilly for non-criminal activity. For any non-espionage activity under investigation, connection to the violation of some underlying criminal law is required. The specter of unfettered investigation of political groups for non-criminal activity is a bogeyman argument unsupported by a realistic appraisal of the law.
9. *See* 50 U.S.C. §1805(a)(3)(B). Title III again has a parallel requirement: probable cause to believe that the facilities are being or will be used for the commission of a domestic criminal offense or are leased to, used by, or listed in the name of the individual suspected of committing the crime. *See* 18 U.S.C. §2518(3)(d).
10. For an articulation of this test, *see Dalia v. United States*, 441 U.S. 238, 255 (1979).
11. *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002).
12. *Id.* at 744.
13. In 1986, Congress added 18 U.S.C. §2518(11) to Title III, authorizing intercept without specification of the particular phone to be intercepted if the interceptee's actions "could have the effect of thwarting interception." *See* Pub. L. No. 99–508, §106(d)(3), 100 Stat 1851 (1986).

"thwart" surveillance) rather than to a particular communications device.[14]

Section 206 authorized the same techniques for foreign intelligence investigations. As the Department of Justice has noted:

> This provision has enhanced the government's ability to monitor sophisticated international terrorists and intelligence officers, who are trained to thwart surveillance by rapidly changing hotels, cell phones, and internet accounts, just before important meetings or communications.[15]

One important safeguard is that the FISA court may authorize such roving wiretaps only if it makes a finding as to the terrorist's actions—that "the actions of the target of the application may have the effect of thwarting the identification" of a terrorism suspect.[16]

The SAFE Act's Unnecessary Burden

The SAFE Act would modify the existing FISA requirements by, in effect, imposing an unreasonable and burdensome ascertainment requirement on law enforcement and intelligence agents. Under the Patriot Act, agents may seek authority for an interception even when the identity of the suspect is not known (so long as probable cause existed to believe the person involved was an agent of a foreign power). The SAFE Act would change that regime. If enacted, it would require agents seeking authority for a wiretap to specify the identity of the target and, if they were unable to do so, to describe with specificity the nature and location of the places where the interception would occur. In other words, in certain circumstances, intelligence agents would be unable to secure a warrant to conduct electronic surveillance because of the indefiniteness of their information.

The proposed modification of the Patriot Act misses the point completely—so much so that one doubts whether any of the authors is a serious student of either law enforcement or intelligence activity. To the extent the SAFE Act calls for specificity with respect to the precise location or facility where the communication is occurring, it is a *non sequitur*. Government agents use roving wiretaps *only* when the location or facility where the communication is occurring is not known with precision—for the simple reason that those under surveillance are attempting to thwart surveillance by constantly changing their location and means of communication. To call for specificity as to location imposes a higher burden on using roving wiretaps in terrorism investigations than in routine domestic criminal investigations.

The SAFE Act's proposal to require that the individual who is the subject of scrutiny be precisely identified is equally foolhardy. In a domestic investigation, the identity of the suspect under scrutiny may often be well-known, though drug dealers do, of course, use aliases. The problem becomes substantially more acute in the shadowy world of espionage and terrorism, where the identity of the investigative subject is often obscured behind a gauze of deceit.

Terrorists change their identity with frequency and often pose as other, real-world individuals. Often, the only description that the intelligence agency will be able to provide to identify the suspect is an alias (or several aliases). Sometimes the description of the terrorism suspect may be nothing more than a physical description. And, on still other occasions, it may consist only of a pattern of behavior (*i.e.*, the person who regularly uses this series of phones, in this order, every third day). To insist that intelligence and law enforcement agents precisely identify the individual under scrutiny or the facility he will be using is, in effect, to ban the use of roving wiretaps in terrorism investigations.

And that is the wrong answer—indeed, the SAFE Act reverses the proper analysis. It imposes a narrow law enforcement paradigm on the efforts to combat terrorism. That paradigm, however, no longer holds. Law enforcement efforts to combat terrorism are policing of a different form: preventative rather than reactive. There is little, if any, value in punishing terrorists after the fact, especially when, in some instances, they are willing to perish in the attack. Hewing to the traditional law enforcement paradigm

14. A number of courts have concluded that the particularity requirements of the Constitution are not violated when roving wiretaps are authorized. *See, e.g.*, *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993).

15. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 3 (2003).

16. 50 U.S.C. §1805(c)(2)(B) (as amended by Section 206 of the Patriot Act).

of particularity in the context of terrorism investigations is a fundamental category mistake.

The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard one or another form of the maxim that "it is better that 10 guilty go free than that one innocent be mistakenly punished."[17] This embodies a fundamentally moral judgment that, when it comes to enforcing criminal law, American society, in effect, prefers to have many more Type II errors (false negatives) than it does Type I errors (false positives).[18] That preference arises, at least implicitly, from a comparative valuation of the social costs attending the two types of error. We value liberty sufficiently highly that we see a great cost in any Type I error. And, though we realize that Type II errors free the guilty to return to the general population, thereby imposing additional social costs on society, we have a common-sense understanding that those costs, while significant, are not so substantial that they threaten large numbers of citizens or core structural aspects of the American polity.

The post–September 11 world changes this calculus, principally by changing the cost of the Type II errors. Whatever the costs of freeing organized crime boss John Gotti or serial murderer John Mohammad might be, they are considered less than the potentially horrific costs of failing to stop the next al-Qaeda assault. Thus, the theoretical rights-protective construct under which our law enforcement system operates must, of necessity, be modified to meet the new reality. We simply cannot afford a rule that "better 10 terrorists be able to succeed in their attacks than that one innocent be mistakenly subject to surveillance."[19] The SAFE Act's proposal to impose a traditional law enforcement construct misses this point altogether.

Nor is there any practical necessity for the SAFE Act's proposed revisions. Though Section 206 has been the law of the land for more than two years, there have be *no* reported instances of abuse of this authority.[20] Whatever else may be said about the Patriot Act, even its most ardent critics must admit that they are basing their legislative proposals on fear rather than reality. But fear is not a basis for policymaking.

Searches and Seizures: Delayed Notification

One section of the Patriot Act that has engendered great criticism is Section 213, which authorizes the issuance of delayed notification search warrants—which critics call "sneak and peek" warrants. Section 3 of the SAFE Act would modify Section 213 by limiting the circumstances in which delayed notification warrants could be issued and by requiring burdensome, repetitive recertification requirements. Section 3 would also sunset (that is terminate) the provisions of Section 213 altogether on December 31, 2005.

Traditional Rules of Search and Seizure

Traditionally, when the courts have issued search warrants authorizing the government's forcible entry into a citizen's home or office, they have required that the searching officers provide contemporaneous notification of the search to the individual whose home or office has been entered.[21] Prior to September 11, some courts permitted limited delays in notification to the owner, when immediate notification

17. *E.g.*, *Furman v. Georgia*, 408 U.S. 238, 367 n. 158 (1972) (Marshall, J., concurring). The aphorism has its source in 4 Blackstone, Commentaries, ch. 27 at 358 (Wait & Co. 1907).

18. "In a criminal case…we do not view the social disutility of convicting an innocent man as equivalent to the disutility of acquitting someone who is guilty…. [T]he reasonable doubt standard is bottomed on a fundamental value determination of our society that it is far worse to convict an innocent man than to let a guilty man go free." *In re: Winship*, 397 U.S. 357, 372 (1970) (Harlan, J., concurring).

19. The closely related point, of course, is that we must guard against "mission creep." Since the justification for altering the traditional assessment of comparative risks is in part based upon the altered nature of the terrorist threat, we cannot alter that assessment and then apply it in the traditional contexts. *See* Paul Rosenzweig & Michael Scardaville, "The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program," at 10–11, Legal Memorandum No. 6, The Heritage Foundation (February 2003) (arguing for use of new technology only to combat terrorism); William Stuntz, "Local Policing After the Terror," 111 Yale L. J. 2137, 2183-84 (2002) (arguing for use of information sharing only to combat most serious offenses).

20. *See supra* n. 3.

would hinder the ongoing investigation. Section 213 codifies that common law tradition and extends it to terrorism investigations. Critics see this extension as an unwarranted expansion of authority—but here, too, the fears of abuse seem to outstrip reality.

Delayed notification warrants are a long-existing crime-fighting tool upheld by courts nationwide for decades in organized crime, drug cases, and child pornography. For example, Mafia Don Nicky Scarfo maintained the records of his various criminal activities on a personal computer, protected by a highly sophisticated encryption technology. Law enforcement knew where the information was—and thus had ample probable cause to seize the computer. But the seizure would have been useless without a way of breaking the encryption. So, on a delayed notification warrant, the FBI surreptitiously placed a keystroke logger on Scarfo's computer. The logger recorded Scarfo's password, which the FBI then used to examine all of Scarfo's records of his various drug deals and murders.[22] It would, of course, have been fruitless for the FBI to have secured a warrant to enter Scarfo's home and place a logger on his computer if, at the same time, it had been obliged to notify Scarfo that it had done so.[23]

The courts have approved this common law use of delayed notification. Over 20 years ago, the Supreme Court held that the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant. The Court emphasized "that covert entries are constitutional in some circumstances, at least if they are made pursuant to a warrant." In fact, the Court stated that an argument to the contrary was "frivolous."[24] In an earlier case—the seminal case defining the scope of privacy in contemporary America—the Court said that "officers need not announce their purpose before conducting an otherwise [duly] authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence."[25]

Section 213 Adopts the Traditional Standard

Section 213 of the Patriot Act thus attempts to codify the common law authority given to law enforcement for decades. As summarized by the Department of Justice:

> Because of differences between jurisdictions, the law was a mix of inconsistent standards that varied across the country. This lack of uniformity hindered complex terrorism cases. Section 213 resolved the problem by establishing a uniform statutory standard.[26]

Now, under Section 213, courts can delay notice if there is "reasonable cause" to believe that immediate notification may have a specified adverse result. The "reasonable cause" standard is consistent with pre–Patriot Act case law for delayed notice of warrants.[27] And the law goes further, defining "reasonable cause" for the issuance of a court order narrowly. Courts are, under Section 213, authorized to delay notice only when immediate notification may result in death or physical harm to an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardize an investigation.

In short, Section 213 is really no change at all; it merely clarifies that a single uniform standard applies and that terrorist offenses are included. Nor does Sec-

21. The requirement has a long-standing provenance in common law. As the King's Bench court said in 1603: "In all cases where the King is a party, the sheriff…may break the party's house, either to arrest him, or to do execution of the King's process, if otherwise he cannot enter. But before he breaks it, he ought to signify the cause of his coming, and to make request to open the doors." *Semanyne's Case*, 5 Co. Rep. 91a, 77 Eng. Rep. 194 (K.B. 1603).

22. *United States v. Scarfo*, 180 F.Supp.2d 572 (D.N.J. 2001).

23. The same, of course, is true of any surreptitious use of listening devices. It would have done little good for the FBI to secure a warrant to enter John Gotti's eating club in Brooklyn to place a recording device in the facility if it had been obliged, at the same time, to politely let Gotti know that he needed to speak clearly into the chandelier, as that was where the bug had been placed.

24. *Dalia v. U.S.*, 441 U.S. 238 (1979).

25. *Katz v. U.S.*, 389 U.S. 347 (1967).

26. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 11 (2003).

27. *See, e.g., United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) (government must show "good reason" for delayed notice of warrants).

tion 213 promise great abuse. Here, as in the past under common law, the officer seeking authority for delayed entry must get authorization for that action from a federal judge or magistrate—under the exact same standards and procedures that apply in getting a warrant to enter a building in the first place. And the law makes clear that in all cases law enforcement must ultimately give notice that property has been searched or seized. The only difference from a traditional search warrant is the temporary delay in providing notification. Here, the presence of oversight rules seems strong—certainly strong enough to prevent the abuse that some critics fear.[28]

Section 213 Has Aided the Fight Against Terrorism

Nor can it be doubted that the delayed notification standards have performed a useful function and are a critical aspect of the strategy of prevention—detecting and incapacitating terrorists *before* they are able to strike.

One example of the use of delayed notification involves the indictment of Dr. Rafil Dhafir. A delayed notification warrant allowed the surreptitious search of an airmail envelope containing records of overseas bank accounts used to ship over $4 million to Iraq. Because Dhafir did not know of the search, he was unable to flee and he did not move the funds before they were seized.[29] In another instance, the Justice Department described a hypothetical situation (based upon an actual case) in which the FBI secured access to the hard drive of terrorists who had sent their computer for repair. In still another, they were able to plant a surveillance device in a building used by terrorists as a safe house.[30]

The SAFE Act Would Needlessly Limit the Use of Delayed Notification Authority

The SAFE Act would make two significant changes to Section 213. First, it would limit the circumstances under which delayed notification would be allowed. Second, it would impose upon the Department of Justice the burden of seeking reauthorization for the delay every seven days, regardless of whether circumstances had changed. Neither change is merited.

The change in standards—limiting the use of delayed notification—is particularly pernicious. Under Section 213 (just as with wiretap or other electronic surveillance) delayed notice is appropriate only when immediate notification may result in:

- Death or physical harm to an individual,
- Flight from prosecution,
- Evidence tampering,
- Witness intimidation, or
- Otherwise seriously jeopardize an investigation.

The SAFE Act would delete this final catchall phrase because it is perceived as too broad and as providing too much leeway for Executive action. But this concern is overly cautious: One can imagine few circumstances in which an investigation would be "seriously jeopardized" that would not also satisfy one of the more specific listings of potential adverse consequences. And nobody disputes that those other consequences (flight, risk of harm, etc.) are appropriate grounds for delay.

Even worse, though, are logical implications of what the SAFE Act would do. Those who would adopt the SAFE Act and delete the catchall phrase are implicitly saying that they are willing to accept the frustration of legitimate investigations. If you advocate changing Section 213, you are advocating the view that, even if an Article III federal judge finds that an investigation *would* be seriously jeopardized without a delay, you will not allow a delay in notification to occur.

In other words, critics value the process of notification more highly than the substance of an impaired investigation. This reverses the more rea-

28. The Department of Justice has reported to Congress that the most common period of delay has been seven days. Delays as short as one day or as long as 90 have been authorized. On occasion, courts have permitted delays for an unspecified period of time lasting until an indictment was unsealed. *See* Letter, Janice E. Brown, Act'g Asst. Atty. Gen., to Hon. James Sensenbrener, Chrmn. House Jud. Comm., Attachment at 10 (May 12, 2003)

29. *See* Letter, William E. Moscella, Asst. Atty. Gen., to Hon. Dennis Hastert, Speaker, at 3 (July 25, 2003); *see also* AP, "Four Indicted for Sending Funds to Iraq" (Feb. 26, 2003) (available at *http://www.chron.com/cs/CDA/printstory.hts/special/iraq/1796320)*.

30. *See* Moscella, Letter to Hastert, at 4.

sonable evaluation of the comparative values, especially when the result is validated by an independent federal judge.

Thus, proponents of the SAFE Act misunderstand the true nature of the issues at stake. The purpose of the notice requirement is twofold: (1) In typical searches, it allows a contemporaneous objection. The individual may say, in effect, "You've got the wrong house." (2) Following notification, it also allows for non-contemporaneous objections to be heard in court so that overzealous execution of the warrant, or a search beyond the scope authorized, may be challenged before a judge.

But in the context of a surreptitious entry and delayed notification, the first of those purposes can have no force. Except by accident, law enforcement or intelligence agents will not conduct a delayed-notice entry in a manner that affords contemporaneous notification—to do so would frustrate the precise purpose of the delayed notification. So the *only* way to effect the first of these two purposes is to prohibit delayed notification entry altogether—a rule that would have very significant costs. And it is equally clear that the second purpose—allowing subsequent challenge in court—is served so long as the law requires (as Section 213 does) eventual notification in all circumstances. The only real argument that critics can make is that Section 213 imposes costs by virtue of the time for which the notification is delayed—a true cost but a comparatively minor one when balanced against the substantial benefits that the process of delayed notification allows in appropriate cases.

The evident utility of the potential uses of Section 213, the provision for subsequent review in court, and the absolute absence of any evidence of abuse of this power suggest that several proposed repeals under congressional consideration are unwise.[31] At worst, they would completely eliminate a long-standing investigative tool for all crimes—both terrorist crimes and traditional common law crimes. At best, the rejection of Section 213 would re-institute a dichotomy between traditional crimes and terrorist investigations—again, a mistaken one that oddly provides greater authority to investigate less threatening common law criminal acts.

Increased Investigative Authority and Business Records

Perhaps no provision of the Patriot Act has excited greater controversy than has Section 215, the so-called angry librarians provision. The section allows the Foreign Intelligence Surveillance Court in a foreign intelligence investigation to issue an order directing the recipient to produce tangible things.

The revised statutory authority in Section 215 is not wholly new. FISA has had authority for securing some forms of business records since its inception. The new statute modifies FISA's original business-records authority in a two important respects:

First, it "expands the types of entities that can be compelled to disclose information. Under the old provision, the FISA court could order the production of records only from 'a common carrier, public accommodation facility, physical storage facility or vehicle rental facility.' The new provision contains no such restrictions."

Second, the new law "expanded the types of items that can be requested. Under the old authority, the FBI could only seek 'records.' Now, the FBI can seek 'any tangible things (including books, records, papers, documents, and other items).'"[32]

Thus, the modifications made by Section 215 do not explicitly authorize the production of library records; but by its terms, it authorizes orders to require the production of virtually any business record. That might include library records, though it would include as well airline manifests, international banking transaction records, and purchase records of all sorts.

Critics of the Patriot Act have decried this provision.[33] As a consequence, Section 4 of the SAFE Act would limit the authority to seek records to those situations where the government can provide "specific and articulable facts" demonstrating that the person to whom the records pertain is the agent of a

31. Besides the SAFE Act itself, repeal proposals are also included in S. 1552 (108th Cong.) (introduced by Sen. Murkowski (R–AK)) and H. Amdt 292 to H.R. 2799 (108th Cong.) (introduced by Rep. Otter (R–ID)) (proposing to prohibit funds to carry out Section 213).

32. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 16 (2003).

foreign power. Section 5 would exempt library Internet services from surveillance that could be carried out on any other Internet system. The proposals are, again, an overreaction to the perception of a problem, mistaking the potential for abuse for the reality.

Section 215 Adopts Traditional Law Enforcement Practices

Section 215 mirrors, in the intelligence-gathering context, the scope of authority that already exists in traditional law enforcement investigations. Obtaining business records is a long-standing law enforcement tactic. Ordinary grand juries for years have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.

For example, in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach. Likewise, in the 1990 Zodiac gunman investigation, a New York grand jury subpoenaed records from a public library in Manhattan. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out books by that poet.[34] In the Unabomber investigation, law enforcement officials sought the records of various libraries, hoping to identify the Unabomber as a former student with particular reading interests.[35]

Section 215 merely authorizes the FISA court to issue similar orders in national-security investigations. It contains a number of safeguards that protect civil liberties.

First, Section 215 requires FBI agents to get a court order. Agents cannot compel any entity to turn over its records unless judicial authority has been obtained. FISA orders are *unlike* grand jury subpoenas, which are requested without court supervision and are subject to challenge only *after* they have been issued.

Second, Section 215 has a narrow scope. It can be used only (1) "to obtain foreign intelligence information not concerning a United States person" or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes, or even domestic terrorism. Nor can it be used in any investigation premised solely on "activities protected by the first amendment to the Constitution."[36]

This is narrower than the scope of traditional law enforcement investigations. Under general criminal law, the grand jury may seek the production of any relevant business records. The only limitation is that the subpoena may be quashed if the subpoena recipient can demonstrate that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[37] There is no necessity of showing a connection to foreign intelligence activity nor any limitation against investigation of United States persons. Thus, unlike under Section 215, the grand

33. "Many [people] are unaware that their library habits could become the target of government surveillance. In a free society, such monitoring is odious and unnecessary…. The secrecy that surrounds section 215 leads us to a society where the 'thought police' can target us for what we choose to read or what Websites we visit." *See* ACLU, "ACLU of New Mexico Seeks to Protect Individual Privacy," Torch, ACLU–New Mexico, July–August 2003. The false image created is, as one writer has characterized it, of "white-haired and apple-cheeked [librarians] resisting as best they can the terrible forces of McCarthyism, evangelical Christian book-burning, middle-class hypocrisy, and Big Brother government." Joseph Bottum, "The Library Lie," The Weekly Standard 7 (Jan. 26, 2004). While politically appealing, the image simply does not match reality.

34. *See* "Patriot Acting Out," Wall St. J. (Jan. 22, 2004). The original source for this information is: *Myth vs. Reality* at 14.

35. *See* James Richardson and Cynthia Hubert, "Unabomber used library at UC Davis?" Sac. Bee (April 10, 1996) (available at *http://www.unabombertrial.com/archive/1996/041096-1.html*) (reporting that UC Davis library provided book to FBI with markings relating to Unabomber manifesto); *cf.* Patrick Hoge, "Rural acquaintances say Kaczynski attracted little notice," Sac. Bee. (April 5, 1996) (available at *http://www.unabombertrial.com/archive/1996/040596-2.html*) (reporting on Kaczynski's reading habits at library in Montana). Some courts have interpreted their State constitutions to provide a First Amendment protection that does not exist in federal law. *See, e.g., Tattered Cover Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002).

36. 50 U.S.C. §1861(2)(B).

37. *United States v. R. Enterprises*, 498 U.S. 292, 301 (1991).

jury may inquire into potential violations of *any* federal crime with effectively limitless authority.[38]

Criticism of Section 215 Is Misguided

Critics make two particular criticisms of this provision: that the judicial review it provides for is a chimera, and that the provision of Section 215 imposing secrecy on the recipients of subpoenas issued pursuant to the section imposes a "gag rule" that prevents oversight of the use of the section's authority. Neither criticism, however, withstands close scrutiny.

Section 215 provides for judicial review of the application for a subpoena for business records. The language provides, however, that upon application, the court "shall" issue the requested subpoena. From the use of the word "shall," critics infer that the obligation to issue the requested subpoena is mandatory and, thus, that the issuing court has no discretion to reject an application. Of course, if this were true (which, as discussed below, it is not), then the absence of any judicial ability to reject an application would reduce the extent of judicial oversight.

But critics who make this argument (even if it were the case) miss the second-order effects of judicial review. It imposes obligations of veracity on those seeking the subpoenas, and to premise an objection on the lack of judicial review is to presuppose the mendacity of the subpoena affiants. It is also to presuppose the absence of any internal, administrative mechanisms in order to check potential misuse of the subpoena authority. And, most notably, it presupposes that the obligation to swear an oath of truthfulness, with attendant perjury penalties for falsity, has no deterrent effect on the misuse of authorities granted.[39]

But even more significantly, this criticism misreads the statute, which, while saying that the subpoena "shall" issue, also says that it shall issue as sought *or* "as modified." The reviewing judge thus explicitly has authority to alter the scope and nature of the documents being sought—a power that cannot be exercised in the absence of substantive review of the subpoena request. Thus, the suggestion that the provisions of Section 215 preclude judicial review is simply mistaken. To the contrary, Section 215 authorizes judicial review and modification of the subpoena request which occurs before the subpoena is issued. This is a substantial improvement over the situation in traditional grand jury investigations where the subpoena is issued without judicial intervention and the review comes, at the end, only if the subpoena is challenged.

Nor is judicial oversight the only mechanism by which the use of Section 215 authority is monitored. The section expressly commands that the Attorney General "fully inform" Congress of how the section is being implemented. On October 17, 2002, the House Judiciary Committee, after reviewing the Attorney General's first report, indicated that it was satisfied with the Justice Department's use of Section 215: "The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."[40] If it were—if, for example, the Department were conducting investigations based upon the reading habits of suspects, in violation of the First Amendment—we can be sure that Congress would have said so. That it has not demonstrates that, once again, critics' fears far outpace reality.[41]

The second criticism—that Section 215 imposes an unwarranted gag rule—is equally unpersuasive. Sec-

38. A "United States person" is defined in Exec. Order 12333 part 3.4 as "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States…."

39. For a similar point, *see* Daniel Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 S. Cal. L. Rev. 1083, 1124–28 (2002) (highlighting the significance of judicial oversight and warrant requirements in maintaining an "architecture of power" to protect privacy). Warrants raise the "standard of care of law enforcement officials by forcing them to document their requests for authorization" and the "requirement of prior approval prevents government officials from dreaming up post-hoc rationalizations." *Id.* at 1126–27. This provides an institutional/procedural check on abuse even if we assume that magistrates routinely defer to police and prosecutors.

40. *See* Statement of F. James Sensenbrenner, Jr. Chmn. House Jud. Comm (Oct. 17, 2002) (available at *http://www.house.gov/judiciary/news101702.htm*).

41. Indeed, they have ignored General George Patton's dictum: "Do not take counsel of your fears." *See* George S. Patton, Jr., *War as I Knew It* (Bantam 1989). Patton was repeating a sentiment originally attributed to General Stonewall Jackson.

tion 215 does prohibit recipients of subpoenas from disclosing that fact—a precaution that is necessary to avoid prematurely disclosing to the subjects of a terrorism investigation that they are subject to government scrutiny. That prohibition might be independently justified, given the grave nature of the potential threats being averted.

But it need not be—for, again, the secrecy provisions of Section 215 merely extend existing rules in traditional law enforcement grand juries to the more sensitive intelligence arena. In the grand jury context, it is common for custodians of third-party records to be prohibited from disclosing the existence of the document request. Banks, for example, may be obliged to conceal requests made to them.[42] And it is clear, beyond peradventure, that these grand jury secrecy obligations are constitutional. For example, when the nanny of JonBenet Ramsey was called to testify before a state grand jury, state law prohibited her from disclosing the substance of her testimony. When she challenged that law (on the ground that it infringed her freedom of speech), her challenge was rejected by the courts.[43]

The SAFE Act Would Hobble Section 215

The SAFE Act proposes to require a showing of "specific and articulable facts" before a Section 215 order may be issued. That showing would impose a greater obligation on law enforcement in an intelligence investigation than under the simple "relevance" standard that applies to federal grand juries investigating ordinary criminal offenses. The purpose of the non-intrusive records request is precisely to develop the specific and articulable facts that warrant a greater intrusion, for if specific and articulable facts to seek the records exist, police will have sufficient probable cause to execute a search warrant—and under warrant there is less possibility that the required records will be destroyed.

In other words, the balance between the standard and the degree of intrusion is a tradeoff: The lesser the standard law enforcement must meet, the lesser the intrusion permitted. By altering that balance, the SAFE Act will have the perverse effect of providing law enforcement with the incentive to prefer more intrusive means.

In short, critics of Section 215 make a very difficult and, in the end, unpersuasive argument. They offer the view, in effect, that traditional law enforcement powers that have been used in grand juries for years to investigate common law crimes and federal criminal offenses ought not to be used with equal authority to investigate potential terrorist threats. To many, that argument seems to precisely to reverse the evaluation—if anything, the powers used to investigate terrorism, espionage, and threats to national security ought to be greater than those used to investigate mere criminal behavior.[44]

This is not, of course, to denigrate the significance and seriousness of many federal and state crimes; but it is to recognize that, however grave those crimes are, they do not pose the same risk to the foundations of American society or to the security of large numbers of citizens as the risks posed by potential terrorist acts.

Consideration of Section 215 should be grounded in a solid understanding of what the section actually authorizes.[45] It should not be swayed by the public mythology that surrounds this provision. That myth has led to the rather absurd result that some librarians are destroying their borrowing records to prevent them from becoming available to the federal government.[46] In other words, those charged in our society with protecting and maintaining knowledge and information are destroying it. The interest in protecting civil liberties must be high—but not so high that we lapse into hysteria.[47]

Conclusion

The Patriot Act has become something of a political football in the past few months. One sees television commercials of anonymous hands ripping up

42. 12 U.S.C. §3604(c).

43. *Hoffmann-Pugh v. Keenan*, 338 F.3d 1136 10th Cir. 2003); *see also Hoffman-Pugh v. Ramsey*, 312 F.3d 1222 (11th Cir. 2002) (rejecting libel suit filed by nanny against the Ramsey family).

44. This view is not an idiosyncratic one. At the time the Patriot Act was passed, Senator Biden (D–DE) argued that "the FBI could get a wiretap to investigate the mafia, but they could not get one to investigate terrorists. To put it bluntly, that was crazy! What's good for the mob should be good for terrorists." Cong. Record at S11048 (Oct 25, 2001) (available at *http://www.lifeandliberty.gov/subs/support/senbiden102501_1.pdf*), *quoted in* Barbara Comstock, "Prez Calls Dems Patriot Games Bluff," Nat'l Review Online (Jan. 21, 2004) (available at *http://www.nationalreview.com/comment/comstock200401211300.asp*).

the Constitution, with a voice-over blaming Attorney General John Ashcroft. Print ads show an elderly gentleman leaving a bookstore with text decrying the use of government powers to get his book purchase list. But the hysteria is based on false premises.

We cannot decide policy based upon an overwrought sense of fear. Most of the steps proposed to combat terrorism were previously used to combat organized crime. And there is no evidence of any real abuse. No First Amendment liberties have been curtailed, no dissent or criticism suppressed.[48] While we must be cautious, John Locke, the 17th century philosopher who greatly influenced the Founding Fathers, was right when he wrote:

> In all states of created beings, capable of laws, where there is no law there is no freedom. For liberty is to be free from the restraint and violence from others; which cannot be where there is no law; and is not, as we are told, a liberty for every man to do what he lists.[49]

Thus, the obligation of the government is a dual one: to protect civil safety and security against violence *and* to preserve civil liberty.

In reviewing our policies and planning for the future, we must be guided by the realization that this is not a zero-sum game. We can achieve both goals—liberty and security—to an appreciable degree. The key is empowering government to do the right things while exercising oversight to prevent the abuse of authority. So long as we keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on our fundamental liberties can be avoided.

—Edwin Meese III is Ronald Reagan Distinguished Fellow in Public Policy and Chairman of the Center for Legal and Judicial Studies at The Heritage Foundation. Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies and Adjunct Professor of Law at George Mason University School of Law.

45. Critics of Section 215 do, however, have one strong argument against renewal of the Section 215 authority (which sunsets in December 2005)—that the authority granted may be unnecessary. Facing wide public criticism of the provisions of Section 215, the Attorney General has disclosed that, at least as of September 2003, the provision had not been used to secure any records. *See* Memorandum for Director Robert S. Muller (Sept. 18, 2003) (available at *http://www.cdt.org/security/usapatriot/030918doj.shtml*). But it is important to recognize that this is a question of *utility*, not a question of *abuse*. And we know that the September 11 terrorists did use Internet connections at libraries to communicate, well prior to the existence of any predication that they had committed a crime. *See*, *e.g.*, Farhad Manjoo, "Terrorists Leave Paperless Trail," Wired News (Sept. 20, 2001) (available at *http://www.wired.com/news/politics/0,1283,46991,00.html*). Thus, the potential utility of the section exists and the suggestion in the SAFE Act to unilaterally and prematurely exempt library Internet connections from surveillance is most unwise.

46. *See*, *e.g.*, Sen. Russ Feingold, Speech on the Libraries, Bookseller and Personal Records Privacy Act (Mar. 7, 2003) (available at *http://feingold.senate.gov/speeches/03/07/2003811915.html*) (reporting such events); "ACLU of Florida Urges Libraries to Warn Patrons of Government's New Domestic Spying Powers Under the USA Patriot Act" (July 30, 2003) (available at *http://www.aclufl.org/body_section215release.html*) (same).

47. As former Attorney General Meese has noted, the position adopted by librarians is particularly odd when contrasted with their long-standing opposition to federal provisions restricting children's on-line access to pornography. It is at least a little jarring that librarians see it as their duty to protect the access of minors to pornography while denying the government access to information of national security importance. *See* NBC News: Today (Sept. 30, 2003) (transcript available at 2003 WL 55607752). The American Library Association has also declined to condemn Fidel Castro's jailing of librarians. *See* Nat Hentoff, "Carrying Fidel's Water," Wa. Times at A19 (Jan. 26, 2004).

48. *See* Michael Chertoff, "Law, Loyalty, and Terror," The Weekly Standard 15, 16 (Dec. 1, 2003) (making this claim). Critics can point to little, if any, evidence rebutting this assertion.

49. John Locke, *Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988), 305.