Federalist Society for Law and Public Policy Studies

White Paper on Anti-terrorism Legislation
Intelligence and the New Threat:
The USA PATRIOT Act and Information Sharing Between the Intelligence and Law Enforcement Communities

Prepared by:

Brian H. Hook
Margaret J. A. Peterlin
Peter L. Welsh

December, 2001

The New Threat and the Need for Enhanced Intelligence

The nature of the threat to United States national security and, especially, the nature of the threat posed by terrorist operations has changed fundamentally in the past decade. Shortly after the September 11 attacks, Ambassador Paul Bremer, who headed the National Commission on Terrorism, observed that "[t]he threat of terrorism is changing dramatically. It is becoming more deadly and it is striking us here at home."[1] Contemporary terrorism traces its roots to the acts of political violence, such as the murder of eleven Israeli athletes at the Munich Olympics in 1972, committed in Western Europe during the late 1960s and 1970s. However, as Ambassador Bremer argues, today's terrorists have little in common with the pragmatic terrorists of the Cold War era.[2]

Much of the terrorist activity during the 1960s and 70s was inspired by Marxist-Leninist ideology, and the terrorists who acted in furtherance of that ideology did so principally to draw attention to their cause and gain certain worldly political concessions. These groups also were motivated by secular rather than apocalyptic ends. For example, they sought to drive the United States out of Western Europe, to compel Britain to withdrawn from Northern Ireland or to undermine NATO.[3] By gaining attention through terrorist acts, the old school of terrorists believed that they could increase support among the general public in the West for their ideology. Moreover, these groups were quick to claim responsibility for a terrorist attack and would often release a document seeking political concessions consistent with Marxist ideology. By proceeding with the purpose of persuading the public in the West of the rightness of their cause and commending its widespread adoption, these early terrorist groups were necessarily constrained in the level of terror they could inflict. By inflicting human casualties, earlier terrorist groups ran the risk of alienating people from their cause. They, therefore, adopted certain limitations on the destruction they were prepared to inflict.[4] As Ambassador Bremer has noted, "[t]here was a self-constraint built into the terrorists' acts and the number of casualties they were willing to inflict."[5]

---

[1] L. Paul Bremer III, *Testimony Before the Senate Select Committee on Intelligence* (June 8, 2000).

[2] *Id*.

[3] The Baader-Meinhoff group in Germany, Action Directe in France, the Red Brigades in Italy, the Irish Republican Army, and the Palestine Liberation Organization were all animated by such practical agendas.

[4] It also bears emphasizing that these terrorist groups only threatened Americans when they were outside the country.

[5] L. Paul Bremer III, *Speech to the Heritage Society* (July 12, 2000).

The predominate terrorist threat today comes from militant Islam. Of the 19 Foreign Terrorist Organizations published by the State Department, ten are Islamic organizations.[6] The groups that have launched the terrorist campaign against America are driven by a profound hatred of Western religion and Western civilization. These terrorists are not, moreover, motivated principally by pragmatic political goals. In the words of Ambassador Bremer, "[t]hese men do not seek a seat at the table; they want to overturn the table and kill everybody at it."[7] As such, they are not amenable to calculated or deterrent measures. Islamic terrorists have defined a mode of total war in which their military inferiority to the West is overcome by an indirect confrontation with the West. This strategy was detailed in *The Quranic Concept of War*, published in 1979 by S.K. Malik, a militant Pakistani brigadier.[8] Arguing in favor of terror as a strategy for war, Malik writes, "Terror struck into the hearts of the enemies is not only a means, it is the end in itself. Once a condition of terror into the opponent's heart is obtained hardly anything left is to be achieved. It is the point where the means and ends meet and merge. Terror is not a means of imposing decision upon the enemy; it is the decision we wish to impose upon him."[9] Today's terrorists are opposed to Western liberalism, as such, and seek the de-stabilization or destruction of pro-Western governments.[10]

The threat from escalating terrorist attacks is also an imminent one. As Yossef Bodansky argues in his biography, *Bin Laden*, Islamic extremists are "determined to ensure that [the] malaise that had already destroyed Christendom did not penetrate and similarly corrupt and destroy the modern world. All means, including the use of violence and terrorism, were justified to prevent such corruption."[11] Given the eagerness with which certain Islamic terrorists are seeking weapons of mass destruction, moreover, there evidently is not sufficient time for liberal

---

[6] Abu Sayyaf Group; Armed Islamic Group; Hamas; Harakat ul-Mujahidin; Hizballah; Islamic Group; Islamic Movement of Uzbekistan; Al-Jihad; Palestinian Islamic Jihad; and Al-Qaeda. State Department Publication, Foreign Terrorist Organizations, released 2001.

[7] L. Paul Bremer III, "A New Strategy for the New Face of Terrorism," *National Interest*, No. 65-S, p. 24 (Thanksgiving 2001)

[8] S.K. Malik, *The Quranic Concept of War* (Quoted in Yossef Bodansky, *Bin Laden*, p. XV (Roosevelt, CA: Prima Publishing 1999)).

[9] *Id*.

[10] *See e.g.* Norman Podhoretz, "Israel Isn't the Issue," *Wall Street Journal*, September 20, 2001.

[11] The Ayatollah Kohmeini popularized the view in the Muslim world that America is oriented principally around money-making and that such an orientation, according to Khomeini, makes "prostitution [the] community's way of life." One follower of Khomeini's described America as "a collection of casinos, supermarkets, and whore-houses linked together by endless highways passing through nowhere." *Quoted in* Bodansky, *Bin Laden* at XIII. Accordingly, Islamic fundamentalists have long sought an end to what they consider unjust occupation of Muslim lands by those who they view as corrupt Westerners.

democratic mores to counteract extremist Islam.[12] The current circumstances, by and large, rule out proceeding by political or diplomatic half-measures.

Combating such a network presents entirely new challenges to Western governments and to the intelligence and law enforcement communities in the West. Because of the need to defend on all fronts against a terrorist attack, homeland security has an unusually great need for highly efficient and sophisticated intelligence and law enforcement operations. Ambassador Bremer explains,

> The terrorists take advantage of two important asymmetries. First, in the fight against terrorism, defenders have to protect all of their points of vulnerability around the world; the terrorist has only to attack the weakest point. This lesson was brought home to the U.S. government when Al-Qaeda attacked the American embassies in Nairobi and Dar es-Salaam in August, 1998, two embassies thought to be in little danger and, thus, ill-protected. Secondly, the costs of launching a terrorist attack are a fraction of the costs required to defend against it. To shoot up an airport, a terrorist needs only an AK-47 assault rifle; defending that same airport costs millions of dollars. The September 11 attacks probably cost less than $2 million and caused over $100 billion in damage and business disruption. Thus, the new terrorism reverses the conventional wisdom that, in military operations, the offense must be three time as strong as the defense. How, then, are we to fight this new and increasingly dangerous threat? The proper objective of a counter-terrorist policy is to prevent attacks before they happen. So, more than in any other field of foreign and national security affairs, success in the fight against terrorism depends on having good intelligence.[13]

Gaining and making effective use of "good intelligence" against this new threat, moreover, requires a change in the operational structure of intelligence and law enforcement agencies as well as more effective modes of cooperation between the agencies.

Many have argued -- even before the events of September 11 -- that the intelligence and law enforcement communities are not institutionally capable of meeting the new terrorist threat. Just one month before the World Trade Center bombing, for example, a CIA veteran who spent nine years in the Directorate of Operations for the Middle East wrote in the *Atlantic Monthly* that "Westerners cannot visit the cinder-block, mud-brick side of the Muslim world—whence bin Ladin's foot soldiers mostly come—without announcing who they are. No case officer stationed in Pakistan can penetrate either the Afghan communities in Peshawar or the Northwest Frontier's numerous religious schools, which feed manpower and ideas to bin Ladin and the Taliban, and seriously expect to gather useful information about radical Islamic terrorism—let alone recruit foreign agents."[14] Another CIA veteran pointedly identified a related problem: "The CIA

---

[12] *See e.g.* Paul A. Rahe, *Republics: Ancient and Modern*, Vol. 2, pp. 85-104 (Chapel Hill: University of North Carolina Press 1994).

[13] Bremer, "A New Strategy for the New Face of Terrorism," *supra* note 7 at 25.

[14] Reuel Marc Gerecht, "The Counterterrorist Myth," *The Atlantic Monthly*, July/August 2001.

probably doesn't have a single truly qualified Arabic-speaking officer of Middle Eastern background who can play a believable Muslim fundamentalist who would volunteer to spend years of his life with shitty food and no women in the mountains of Afghanistan. For Christ's sake, most case officers live in the suburbs of Virginia. We don't do that kind of thing."[15]

Information sharing between the law enforcement and intelligence communities is especially critical in the new fight against terrorism.[16] Considerable emphasis has recently been placed on the fact that the war on terrorism is precisely that, a war.[17] As Ambassador Bremer argues, intelligence is crucial to winning this war on terrorism. But so, too, is law enforcement. Indeed, the on-the-ground fight against terrorism has much in common with a criminal investigation. In fighting this war, the U.S., by and large, is not engaging an enemy that is massed on a battlefield and that may be defeated by conventional forces utilizing standard wartime intelligence capabilities. It is not sufficient to destroy and/or confiscate the enemy's battlefield capabilities and disperse its troops. Rather, rooting out the secretive, diffuse cells of today's terrorists – particularly, those that may remain in the United States -- requires tactics that are similar to those employed in certain criminal investigations. The neutralization of the threat posed to those cells may involve the arrest of the individuals involved. The intelligence and law enforcement communities must, therefore, work together with a level of coordination not previously achieved in the history of the two communities.

Brief History of Interagency Information Sharing

The USA PATRIOT Act promotes greater cooperation and information sharing between the intelligence and law enforcement communities. In doing so, the PATRIOT Act does not overturn the *status quo ante* with respect to coordination between intelligence and law enforcement. Although restricted in certain particular respects (such as grand jury secrecy, for example) and often plagued by political infighting and bureaucratic inefficiencies, there is nevertheless a long history in America of cooperation and information sharing between the CIA and the FBI.[18] The PATRIOT Act, moreover, does not change qualitatively the law or policy with regard to cooperation or information sharing between the law enforcement and intelligence communities. The relevant provisions of the PATRIOT Act are consistent with pre-existing law. Indeed, most of the provisions of the PATRIOT Act have generally been in effect by executive

---

[15] *Id*.

[16] Bremer, "A New Strategy for the New Face of Terrorism," *supra* note 7 at 25.

[17] *See e.g.* "Getting Serious," *Wall Street Journal*, September 13, 2001; Douglas W. Kmiec, "War Crimes Are Different," *Wall Street Journal*, November 15, 2001.

[18] *See e.g.* Edward Jay Epstein, *The Assassination Chronicles: Inquest, Counterplot and Legend* (New York: Carrol & Graf 1992); Curt Gentry, *J. Edgar Hoover: The Man and His Secrets*, p. 418 (New York: Plume 1991); *Final Report of the Select Committee to Study* Governmental Operations with Respect to Intelligence Activities, Vol. 1, p. 440 (Washington DC: GPO 1976)(herein the "Report of the Church Committee").

order for at least twenty years.[19] What the PATRIOT Act principally seeks to correct is the bureaucratic friction that has too often existed between these two agencies.[20]

Origins of the Separation of Law Enforcement and Intelligence

The law enforcement and intelligence functions of the United States have, for the most part, been allocated between the Federal Bureau of Investigation, on the one hand, and the Central Intelligence Agency, National Security Agency, and military intelligence organizations, on the other hand. The separation between the law enforcement and intelligence communities was established partly out of a concern for protecting civil liberties but significantly as a result of bureaucratic compromises.

Originally called simply the Bureau of Investigations, the Federal Bureau of Investigation was established in 1908 by Attorney General Charles Joseph Bonaparte. The Bureau of Investigations came into its own during the First World War when it coordinated attempts to infiltrate and suppress radical organizations, such as the International Workers of the World movement.[21] The FBI's formal intelligence-gathering efforts were, moreover, started shortly thereafter in the immediate wake of several terrorist acts committed by certain of these same radical groups in the summer of 1919.[22] In response to those attacks, the Bureau of Investigations started the General Intelligence Division which was formally organized on August 1, 1919 and headed from the outset by the young J. Edgar Hoover.[23] In the ensuing years, the General Intelligence Division developed into extensive and sophisticated counter-intelligence operation.[24]

By the end of the Second World War, the FBI was engaged in significant efforts to combat foreign espionage both at home as well as abroad.[25] The FBI's counterintelligence

---

[19] *See* "United States Intelligence Activities," Executive Order 12333 (December 3, 1981).

[20] *See* Gentry, *supra* note 17, at 410 *ff*.; *see also* Stewart Baker, "Dangerous Secrets," *Wall Street Journal*, October 5, 2001 ("[T]he grand jury rules have the effect putting Justice in a position of primacy among the agencies. [Prior to passage of the PATRIOT Act] the Justice Department [could] make exceptions to the no-sharing rule, but only for CIA analysts who agree to work as prosecutors' assistants, and so long as prosecutorial goals take precedence over intelligence ones.").

[21] Gentry, *supra* note 17, at 70 *ff*.

[22] *Id*.

[23] *Id*.

[24] Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century*, pp.134*ff*. (New York: The Free Press 1992).

[25] *Id*.

efforts, while conducted mostly by means of law-enforcement tactics, were nevertheless far-reaching in scope.[26] One of the FBI's main counterintelligence functions during the post-Second World War era, for example, was the "surveillance of hostile foreign diplomats and their premises."[27] Given the breadth of the FBI's post-war counter-espionage efforts, moreover, conflicts with the other intelligence agencies – especially, the newly-formed National Intelligence Authority (precursor to the NSA) and Central Intelligence Group (precursor to the CIA), -- were inevitable.[28] In 1946, J. Edgar Hoover attempted to persuade President Truman to place the nascent Central Intelligence Group under the direct control of Hoover and the FBI.[29] Truman, however, refused.[30] The President explained to others, at the time, that he did not want to place one man (particularly, J. Edgar Hoover) in charge of law enforcement and domestic and foreign intelligence.[31]

Although concerns about placing the main federal law enforcement and intelligence powers in the hands of one person account, in part, for the modern day division of authority between the FBI and the CIA, those concerns do not suggest that information sharing or coordination between the FBI and the CIA pose any threat to civil liberties. As Angelo Codevilla has argued, "[i]n realty and contrary to conventional wisdom, the CIA has *no* weapons with which to threaten civil liberties. The FBI, not the CIA, has the power of arrest. The FBI, not the CIA, can work with federal and state prosecutors,. Nevertheless, the myth that the division of responsibility for [counterintelligence] has something to do with safeguarding civil liberties is an enduring one."[32] Rather than serving a legitimate concern for the protection of civil liberties, Codevilla has suggested that the separation of the intelligence and law enforcement communities was, in some significant part, the result of "a series of bureaucratic compromises" and that the stakes in the ensuing struggles "were simply pieces of bureaucratic turf."[33]

---

[26] *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Report of the Committee on the Role and Capabilities of U.S. Intelligence, Appendix, p. A-4 (Washington DC: GPO March 1, 1996); *see also* Codevilla, *supra* note 23, at 136.

[27] *Id*.

[28] Gentry, *supra* note 17, at 326-7.

[29] *Id*.

[30] *Id*.

[31] *Id.*; *cf*. *Report to the President by the Commission on CIA Activities within the United States*, p. 11 (Washington D.C.: GPO 1975) (herein the "Report of the Rockefeller Commission").

[32] Codevilla, *supra* note 23, at 136.

[33] *Id*.

The allocation of the pieces of bureaucratic turf between the law enforcement and intelligence communities has occurred in several stages during the post-war era. There are at least three stages to this process: (1) the establishment of the Central Intelligence Agency and the National Security Agency in 1947; (2) the Church Committee; and (3) the Reagan administration.

The Post-war Era – The National Security Act of 1947

The CIA and NSA were established as separate government agencies with passage of the National Security Act of 1947. The Act, moreover, includes the original mandate granted to the Director of Central Intelligence.[34] Notably, Section 103-3 of the National Security Act, specifying the "Responsibilities of Director of Central Intelligence," provides, in relevant part, that the Director of Central Intelligence shall, "collect intelligence through human sources and by other appropriate means, except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions."[35] The term "internal security functions" has no clear meaning under the Act and the term has been used liberally by critics of the CIA to attempt to limit the agency's powers.[36] At least one source has stated that "[t]he statutory language regarding the authorities and functions of the new Central Intelligence Agency was left intentionally vague. In part this reflected the bureaucratic sensitivities involved in specifying in the law the DCI's roles and missions in regard to other agencies, and, in part, the desire to avoid wording that other governments might find offensive."[37]

The Turmoil of the 1970s -- The Rockefeller Commission and Church Committee

Certain high profile cases involving domestic intelligence gathering, and subsequent political scrutiny of those cases, have further defined the post-war allocation of power between the CIA and FBI. In June of 1975, the Commission on CIA Activities Within the United States, also known as the Rockefeller Commission, released its final Report to the President. Shortly thereafter, the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, known as the Church Committee (after its Chairman, Senator Frank Church) released its report on the CIA.[38] The Rockefeller Commission and Church Committee reports detailed a number of activities which both reports characterized as abuses of the CIA's statutory authority. For example, the Rockefeller Commission found that, between 1952 and 1973, the CIA conducted a mail intercept program which involved the U.S. government opening

---

[34] *See* 50 U.S.C. 403 *et seq*.

[35] 18 U.S.C. ' 403-3.

[36] *See e.g. Report of the Rockefeller Commission*, *supra* note 30, at 10-11.

[37] *Preparing for the 21st Century*, *supra* note 25, at p. A-4.

[38] The House Select Intelligence Committee, known as the Pike Committee, conducted a parallel investigation, as well.

thousands of letters sent to and from persons living within the United States.[39] The Commission also found that the CIA established a Special Operations Group to conduct surveillance of American dissident groups.[40] The efforts of the Special Operations Group, dubbed Operation CHAOS, resulted in the collection of significant information and materials on domestic dissident groups.[41] Cold War partisans seized on such abuses of intelligence collection techniques to demonize the CIA. These attacks on the CIA, however, had at least as much to do with the role that the CIA played in its foreign intelligence operations, and how those operations fit within the Cold War political *gestalt*, than with domestic intelligence activities, as such.[42]

More importantly, the Rockefeller Commission and the Church Committee did not rule out information sharing between the law enforcement and intelligence communities and, indeed, recommended *greater* coordination between the CIA and the FBI. Although both the Rockefeller Commission and Church Committee relied on a somewhat simplistic or anachronistic conceptual framework which contemplates that the CIA's activities could be strictly limited to what the Commission frequently refers to as "foreign intelligence matters,"[43] both bodies also acknowledged the need for some significant measure of coordination between the law enforcement and intelligence communities. Indeed, the Church Committee observed that there has been a long history of coordination between the CIA and FBI and recommended still closer coordination between the agencies, especially in their counterintelligence efforts:[44]

> *Coordination between CIA and FBI counterintelligence units is especially critical*. The history of CIA-FBI liaison has been turbulent, though a strong undercurrent of cooperation has usually existed at the staff level since 1952 when the Bureau began sending a liaison person to the CIA on a regular basis. The sources of friction between the CIA and FBI in the early days revolved around such matters as the frequent

---

[39] *Report of the Rockefeller Commission, supra* note 30, at 20-21.

[40] *Id*. at 23-4.

[41] *Id*; *see also Report of the Church Committee*, *supra* note 17, at 436.

[42] *See e.g.* "Unspooking Spooks," *Wall Street Journal*, September 18, 2001; Tom Clancy, "How We Got Here" *Wall Street Journal*, September 18, 2001.

[43] Notably, the Report of the Rockefeller Commission recommends that Section 403 of the National Security Act be amended to "[m]ake explicit that the CIA's activities must be related to *foreign* intelligence." *Report of the Rockefeller Commission, supra* note 30 at 12. In so recommending, the Commission lost sight of the fact, that the CIA has an important role to play in domestic *counterintelligence*.

[44] The focus of counterintelligence is on developing capabilities to thwart clandestine threats to national security. *See* Abraham N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 2d ed. (Washington DC: Brassey's 1993). Counter-terrorism is closely analogous to, and arguably, subsumed within counterintelligence. *See* Executive Order 12333, *supra* note 18 at ' 3.4(a).

> unwillingness of the Bureau to collect positive intelligence for the CIA within the United States or to help recruit foreign officials in this country. In 1970 an essentially minor incident resulted in an order from FBI Director Hoover to discontinue FBI liaison with the Central Intelligence Agency. Although informal communications between CIA and FBI staff personnel continued, it was not until the post-Hoover era that formal liaison relations were reestablished. *Today, there is still a need for closer coordination of FBI and CIA counterintelligence efforts.*[45]

The Rockefeller Commission's Report, moreover, observed that the National Security Act, "was intended to promote coordination, not compartmentation [sic] of intelligence between government departments."[46] In addition, the Commission's report states that "legitimate domestic CIA activities occasionally cross the path of FBI investigations. Daily liaison is therefore necessary between the two agencies."[47] The Commission also recommends that, "[t]he Director of Central Intelligence and the Director of the FBI should prepare and submit for approval by the National Security Council a detailed agreement setting forth the jurisdiction of each agency and providing for effective liaison with respect to all matters of mutual concern."[48]

The Reagan Era

Much of the information sharing policy embodied in the USA PATRIOT Act has been in effect for at least twenty years pursuant to an Executive Order issued by President Reagan. In December of 1981, President Reagan issued Executive Order 12333 on "United States Intelligence Activities." Executive Order 12333 was intended to clarify the relationship among the various intelligence agencies of the United States Government. The Order includes as one of its goals "to the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort."[49] The Order contains many of the same policies embodied in the PATRIOT Act. For example, the Order provides that the Director of Central Intelligence shall, "coordinate foreign intelligence and counterintelligence relationships between agencies of the Intelligence Community and the intelligence or internal security services of foreign governments, . . .".[50] The Order further provides that the collection by the CIA of "foreign intelligence or counterintelligence within the United States shall be

---

[45] *Report of the Church Committee, supra* note 17 at 440 (emphasis added).

[46] *Report of the Rockefeller Commission, supra* note 30 at 22.

[47] *Id*. at 38

[48] *Id*. at 39.

[49] EO 12333, *supra* note 18 at ' 1.1.

[50] *Id*. at ' 1.5. The "Intelligence Community is defined by the Order to include both the CIA and the intelligence elements of the FBI. *See* EO12333, *supra* note 18, at ' 3.4(f).

coordinated with the FBI . . .” and that the CIA shall, “without assuming or performing any internal security functions, conduct counterintelligence activities within the United States in coordination with the FBI.[51] The Order defines both “counterintelligence” and “foreign intelligence” to include gathering information on “international terrorist activities.”[52] The Order also provides that the FBI shall, “[c]onduct counterintelligence activities outside of the United States in coordination with the CIA” and that the FBI shall, “[c]onduct within the United States, when requested by officials of the Intelligence Community designated by the President, activities undertaken to collect foreign intelligence or support foreign intelligence collection requirements of other agencies within the Intelligence Community . . .”.[53]

Information Sharing and the USA PATRIOT Act

The PATRIOT Act's Information Sharing Provisions

Following is a brief overview of the provisions of the PATRIOT Act that relate to information-sharing between the intelligence and law enforcement communities.

- Section 203 – Section 203 of the PATRIOT Act amends Rule 6 of the Federal Rules of Criminal Procedure, governing grand jury secrecy, to permit disclosure of certain information presented before a grand jury. Prior to the PATRIOT Act, law enforcement officials were generally restricted by Rule 6 of the Rules of Criminal Procedure from sharing information provided to a grand jury with members of the intelligence community. While it is important to prevent evidence presented to a grand jury from leaking to the general public, there is little reason to prevent intelligence officials from gaining access to such information on a confidential basis.[54] Section 203 of the PATRIOT Act now permits disclosure of “matters involving foreign intelligence or counterintelligence” occurring before a grand jury to “any Federal law enforcement, intelligence, protective, immigration, national defense or national security official in order to assist the official receiving that information in the performance of his official duties.” The information disclosed may only be used, moreover, “as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.” Section 203 also permits law enforcement to disclose the contents of any wire, oral or electronic communication, or evidence derived therefrom, to any other Federal law enforcement, intelligence, protective, immigration, national defense or national security official.

---

[51] *Id*. at ''1.8(a) and (d).

[52] *Id*. at ''3.4(a) and (d).

[53] *Id*. at '1.14.

[54] *See e.g.* Stewart Baker, “Dangerous Secrets,” *Wall Street Journal*, October 5, 2001.

- Section 901 – Amends section 103 the National Security Act of 1947, which sets forth the DCI's role as head of intelligence, to provide that the Director of Central Intelligence shall provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under the Foreign Intelligence Surveillance Act [FISA] is "disseminated so it may be used efficiently and effectively for foreign intelligence purposes."[55] Section 901 clarifies, however, that the DCI shall have "no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to [FISA] unless otherwise authorized by statute or executive order."

- Section 902 – Clarifies that the definition of the term "foreign intelligence," under the National Security Act shall also include "international terrorist activities." The term "counterintelligence" under the Act already included "international terrorist activities" within its definition.[56]

- Section 903 – States the sense of Congress that "officers and employees of the intelligence community of the Federal Government, acting within the course of their official duties, should be encouraged, and should make every effort, to establish and maintain intelligence relationships with any person, entity or group for the purpose of engaging in lawful intelligence activities. . . ."

- Section 905 – Amends the National Security Act of 1947 to add a new section, titled "Disclosure of Foreign Intelligence Acquired in Criminal Investigations; Notice of Criminal Investigations of Foreign Intelligence Sources." This new section provides, *inter alia*, that "the Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities shall expeditiously disclose to the Director of Central Intelligence . . . foreign intelligence acquired by an element of the Department of Justice or an element of such department or agency, as the case may be in the course of a criminal investigation."

- Section 906 – This section requires that, not later than February 1, 2002, the Attorney General, the DCI and the Secretary of the Treasury jointly submit to Congress a report on the feasibility and desirability of reconfiguring the Foreign Terrorist Asset Tracking Center and the Office of Foreign Assets Control of the Department of Treasury to provide for the "effective and efficient analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations."

---

[55] For more detailed discussion of FISA and changes to FISA effected by the PATRIOT Act, *see* Tom Gede, Montgomery N. Kosma and Arun Chandra, "Developing Necessary and Constitutional Tools for Law Enforcement," Federalist Society White Paper on Anti-Terrorism Legislation: Surveillance and Wiretap Laws, pp.6 *ff*. (November 2001), available at www.fed-soc.org.

[56] 50 U.S.C. 401a(3); *Cf*. Executive Order 12333, *supra* note 18, at ' 3.4(a).

- Section 907 – Requires that no later than February 1, 2002, the Director of Central Intelligence, in consultation with the Director of the FBI, submit to the appropriate committees of Congress a report on the establishment and maintenance within the intelligence community of an element for purposes of producing timely and accurate translations of foreign intelligence to be shared with all other elements of the intelligence community.

- Section 908 – Requires the Attorney General, in consultation with the DCI, to develop a program to provide training to certain officials in the Federal, State and Local governments who are not ordinarily engaged in the collection, dissemination, and use of foreign intelligence. Such training would seek to assist these officials in "identifying foreign intelligence information in the course of their duties, and utilizing foreign intelligence information in the course of their duties, to the extent that the utilization of such information is appropriate for such duties."

These sections represent the main provisions of the Act that allow for increased information sharing. They do not define the limits of the Act's impact on the relationship between the law enforcement and intelligence communities, however. In addition to providing for greater information sharing, for example, the PATRIOT Act also expands many of the FBI's surveillance powers.[57] Any analysis of information sharing must consider the scope and quantity of information shared. Limited sharing presents a different, and perhaps less challenging, question than more-expansive sharing.

Intelligence Collection as Distinguished from Information Sharing

Central to the issue of information sharing between the intelligence and law enforcement communities is how, rather than whether, these communities should share information. Furthermore, of paramount importance is how the information is collected in the first instance, and this shifts the inquiry to one of tracking the use of information and the mechanics and methods of surveillance.[58] As section II demonstrates, the history of intelligence collection has included episodes of overreaching.[59] Even were that not the case, a call for oversight is not inherently an accusation. Rather, it is the civic obligation of both Congress and the citizenry. In our view, the notion that a rule of law is preferred over rule by man properly includes the corollary that scrutinizing that law is not the same as scrutinizing the man.

A wide variety of oversight methods exist to vet intelligence collection, and the Act employs these methods to different degrees and in different contexts. Over time the question will become whether the combination of power granted to the intelligence and law enforcement

---

[57] *See* Gede, Kosma and Chandra, "Developing Necessary and Constitutional Tools for Law Enforcement," *supra* note 62.

[58] *See Id*.

[59] *Report of the Rockefeller Commission, supra* note 30, at 23-4.

communities and the oversight applied have resulted in the proper balance between liberty and security in that same area. This section considers, among the possibilities, three oversight tools as well as a discussion of how those oversight tools were or were not applied to a particular provision of the act.[60] This section also considers how the oversight tools may affect the manner and extent of cooperation between the intelligence and law enforcement communities. The three oversight tools discussed immediately below are judicial involvement, congressional oversight, and sunset provisions.

Since these tools are broadly equivalent, two general considerations are raised. First, each oversight option includes a different accompanying cost. For law enforcement this normally means that the employed option slows the process in some more or less acceptable way.[61] If the process is not slowed, then already strained resources are reprogrammed in order to meet the oversight requirement. These potential drawbacks can be conveniently reduced to two phrases: mission compromise and manpower drain. A third potential drawback is the over-dissemination of sensitive information and the risk of compromising the usefulness of that information.[62] In order to "smoke them out of their holes," we must first discover the location of the hole and then strike when we know they are there.[63] That cannot be done, however, if the terrorists know what we know.[64] These three shape the adaptability of a particular oversight tool to reducing the risk associated with a specific collection technique.

Second, some of the oversight options present standard controversies. For instance, it tends to be the uncommon prosecutor that believes the exclusionary rule does anything more useful than complicate an already unfortunate situation. Another common concern is that congressional oversight rarely occurs.[65] This paper does not address such controversies. Instead, the focus is on the appropriateness of the pairing of the power granted and the oversight tool selected.

---

[60] The last two options, available to the at-large citizenry, were not aspects of particular provisions.

[61] This concern was raised throughout the Conference Committee negotiations.

[62] This concern was raised throughout the Conference Committee negotiations.

[63] President Bush in an interview as reported by CNN. This quote can be viewed at www.cnn.com/2001/us/09/15/bush/terrorism.

[64] This point has been emphasized as recently at December 1, 2001 by Israeli Prime Minister Sharon in an interview with Chris Matthews following another act of war by a group of terrorists, this time the victims were inhabitants and visitors to Zion Square in Jerusalem.

[65] Donald R. Wolfensberger, Dir., The Congress Project Woodrow Wilson Center, *Congressional Oversight: Rules of the Road Less Traveled*, presented before the Oversight Workshop United States Congress on Monday, June 28, 1999 (characterizing Congressional oversight as "the road less traveled" and explaining the political disincentives that keeps it that way.)

Judicial Involvement

The Act's provisions task the judiciary repeatedly. Few of these tasks are new, however. Most of them are mere extensions of a common task to a new item. Some are reductions of the judiciary's role. One example is the involvement of the judiciary in section 209. This section removed stored communications (or yet unopened voicemails) from the definition of "wire communication, " as found in 18 U.S.C. section 2510(1). Previously, law enforcement needed a wiretap order to access stored, unopened email. To some, section 209 rationalizes the treatment of stored voice and non-voice communications. To others, rationality demanded that access to such communications require a wiretap order. If wiretap orders unduly slow the pursuit of information that can be too easily deleted by a potential defendant, then one must look to another of the tools to resolve a lingering concern. Of the remaining options, congressional oversight hearings, FOIA requests, and media coverage are the only practical options. Those with concerns should, moreover, focus their efforts in one of these three areas.

Section 216 authorizes courts to grant pen register and trap and trace orders that are valid nationwide. The controversy surrounding (and nearly consuming) this "Carnivore" provision abated only after a requirement that a complete recording of the information extracted, to include the agents involved, and the configuration of the device during its use would be provided to the relevant judge 30 days after termination of the order. Advocates of the report hope it serves as a bulwark against the improper capture of content under an order that allows only for the capture of addressing information, in the same manner that a trap and trace order for telephones allows only for the capture of dialing information. This report, occurring *ex parte*, does not endanger any classified information and therefore it does not threaten to compromise the mission.

Opponents of the reporting requirement may contend that it is a manpower drain, despite the fact that it appears that the FBI generates the report already and is simply required to provide a copy to the judge. Still, the balance may not yet be ideal. Depending on the duration of the initial trap and trace order a report submitted 30 days after termination may not be sufficient. A more cautious approach would link the interval of the order and the reporting interval. For example, if an initial order is for one year, the reporting requirement could be every three months during the order, with the final report due 30 days after termination. When an initial order is for one month, the final report may be sufficient as the only report. Again, it is impossible to predict whether such an adjustment will be necessary, though it is an option that could improve oversight while remaining sensitive to the mission concerns.

One concern with judicial involvement as an oversight tool relates to the need to contain information. In order to engage clandestine organizations, it is often necessary to have meaningful limits on the use and dissemination of information.[66] The Act sought to correct a too-strict approach. A too-loose approach would lead to an equally ineffectual effort. The first of two possible responses is to limit dissemination by limiting judicial involvement in the process. The second is to limit dissemination through the use of tight controls within the

---

[66] *Countering the Changing Threat of International Terrorism*, Report of the National Commission on Terrorism (Washington DC: GPO June, 2000).

judiciary. A first moderate step may be to require the use of sealed documents before adopting outright limitations on the role of the judiciary.

Congressional Oversight

The Act may rejuvenate the art of congressional oversight. Among the options, congressional hearings may compromise the mission the least. This is because most hearings occur *ex post*. Missions either would be accomplished or abandoned by the time testimony began. That hearings occur after-the-fact also tends to negate the over-dissemination concern. When methods of intelligence gathering are under review, classified hearings are certainly available. Those who malign congressional oversight as ineffectual should consider redirecting their energies to sharpening this tool. The unalterable need for greater information sharing means that the U.S. no longer has the luxury of simply separating law enforcement and intelligence agencies. Separation is a security risk.

Lack of oversight is a potential liberty risk, however. One obstacle to even classified oversight hearings is that they are not costless. While they may not generate the costs associated with mission compromise or over-dissemination, they will be a manpower drain. For those with concerns, this inconvenience is likely to be seen as the exchange for increases in surveillance powers. Members might express impatience when agents or appointees claim unavailability for hearings. This security/liberty pairing means that these agencies must do more on both fronts. The complete obligation to the American people means that the agencies will be responsive to congressional requests and inquiries.

Sunset provisions

The sunset provision applies to many, but not all, of the surveillance provisions of the bill. Interestingly, it does not apply to the controversial section 216, discussed *supra*. The sunset provisions evoked heated negotiations. Having a sunset may mean that law enforcement and intelligence agencies are less likely to realign their bureaucracies as necessary to maximize their information-sharing potential. New operating procedures need to be written, disseminated, and translated into behaviors for the Act to have its intended beneficial result. If agents believe the basis for such efforts will disappear in a short span of time, they may approach the task with an inadequate amount of zeal. Or, more realistically, they may have to rush the process so as to benefit from the provision. Rushed procedures may not be the most secure.

A sunset provision can serve several purposes. First, it has the potential to encourage the good habit of congressional engagement on both sides. Congress has an incentive to discover whether it wants to renew the powers and agencies have an incentive to win renewal. Second, a sunset can be an encouragement for agencies to take additional care in crafting their initial operating procedures. During this period, these careful procedures can become rooted practices. Once rooted, the practices are less likely to change even if the provisions are later made permanent. Ending with the result that additional sunsets are not needed because a sunset was first used. Third, the sunset can be an absolute backstop to any concerns. Legislative inertia works against passage. If the powers prove to be inherently problematic they will most likely expire. Of course, this point loops back to one of the disadvantages of sunsets: inherently helpful powers can also expire.

In comparing these two viewpoints the internal conflict of using a sunset in this circumstance becomes apparent. Several large bureaucracies need to dramatically and quickly alter operational methods while at the same time ensuring that they do so in a careful fashion so as both to accomplish and demonstrate that they remain institutionally sensitive to liberty concerns.

Other Oversight Tools

Beyond the three oversight tools of judicial involvement, congressional oversight, and sunset provisions, there are other options. Lawmakers can apply the exclusionary rule to evidence obtained in a manner that violates the law.[67] This puts the impetus for oversight in the hands of defense attorneys. As mentioned previously, some debate the value of the exclusionary rule. *Mens rea* requirements increase the quality of proof necessary to receive a search warrant or wiretap order. Overreaching is not just less likely, it is less possible, when a judge must be

---

[67] In determining whether to exclude, courts "evaluate the circumstances of [a] case in the light of the policy served by the exclusionary rule...." *Brown v. Illinois*, 422 U.S. 590, 604 (1975). 'The rule is calculated to prevent, not repair. Its purpose is to deter--to compel respect for the constitutional guaranty in the only effectively available way--by removing the incentive to disregard it.... [D]espite its broad deterrent purpose, the exclusionary rule has never been interpreted to proscribe the use of illegally seized evidence in all proceedings or against all persons.' " *Id.* at 599-600 (citations omitted). The exclusionary rule has its limitations ... as a tool of judicial control.... [In] some contexts the rule is ineffective as a deterrent.... Proper adjudication of cases in which the exclusionary rule is invoked demands a constant awareness of these limitations.... [A] rigid and unthinking application of the ... rule ... may exact a high toll in human injury and frustration of efforts to prevent crime. *Terry v. Ohio*, 392 U.S. 1, 13-15 (1968).

Three exceptions to the exclusionary rule have emerged: the independent source exception, the attenuation exception, and the inevitable discovery exception. *People v. LoCicero* (*After Remand*), 453 Mich. 496, 508-509 (1996) (citations omitted). In *Nix v. Williams*, 467 U.S. 431, 442-43 (1984), the United States Supreme Court explained the deterrent purpose of the exclusionary rule, the Court stated:

> The core rationale consistently advanced by this Court for extending the exclusionary rule to evidence that is the fruit of unlawful police conduct has been that this admittedly drastic and socially costly course is needed to deter police from violations of constitutional and statutory protections. This Court has accepted the argument that the way to ensure such protections is to exclude evidence seized as a result of such violations notwithstanding the high social cost of letting persons obviously guilty go unpunished for their crimes. On this rationale, the prosecution is not to be put in a better position than it would have been in if no illegality had transpired. By contrast, the derivative evidence analysis ensures that the prosecution is not put in a worse position simply because of some earlier police error or misconduct.

presented with probable cause that a person *knowingly* contributed money to a terrorist organization.

The next three oversight tools rely on action by the citizenry to be effective. The first creates a civil cause of action for willful disclosures of information that extend beyond what the statute allows.[68] Freedom of Information Act (FOIA)[69] requests provide another opportunity for citizens to educate themselves as to how the agencies are operating. Amendments to FOIA that overreach the legitimate need to restrict access to government records should be resisted. To date, it appears that the Department is evaluating FOIA in light of the present security environment. On October 12, 2001, Secretary Ashcroft released a new FOIA memorandum in which he announced a change in the legal standard the department would use to determine whether it will defend an agency's decision on a particular FOIA request.[70] The last tool needs no greater explanation than simply identifying it: press coverage.

In sum, the mere fact that law enforcement and intelligence agencies are sharing information does not raise concerns. Increased cooperation is necessary to restore security. Hand-in-hand, however, comes the realization that we do not have the luxury of structural separation as an alternative to vigorous oversight. Each relevant group—Congress, the agencies (to include the new office of Homeland Security[71]), and the citizenry—must become more involved in security and more involved in oversight.

CONCLUSION

The coordination and information sharing contemplated by the USA PATRIOT Act between elements of the intelligence community, including the CIA and the FBI, is consistent with existing law governing the activities of law enforcement and the intelligence community.

---

[68] *See* section 223 of the Act.

[69] 5 U.S.C. section 552.

[70] FOIA Post, "*New Attorney General FOIA Memorandum Issued,"* available at www.usdoj.gov/oip/foiapost/2001foaipost19.htm. Under the new standard—sound legal basis—the releasing department's decision will be defended if it is based on a sound legal and factual footing. The previous standard was a "foreseeable harm" standard. These standards should be compared to determine the net effect on the amount of information that is released. Whether a more or less open government is preferred is a normative question for each citizen to answer for himself.

[71] This office should consider including an oversight role as it establishes its procedures. As the central information clearinghouse, based on a flow chart created by the administration, this office may be in a good position to monitor the monitors. Additionally, the executive branch may consider altering the executive order that modeled the office after the National Security Council; Thomas Ridge, serving in the same capacity as National Security Adviser Condoleezza Rice, is not a Cabinet secretary and is not required to appear before Congress. *See* Preston, Mark "*Ridge Rebuffs Hill Requests,"* Roll Call, November 5, 2001.

America's history includes periods of cooperation and information sharing between the CIA and the FBI. In addition, although the method by which government officials conduct surveillance and gather information has significant implications on civil liberties, the simple sharing of information between two elements of the intelligence community, or between the intelligence community and the law enforcement community, does not implicate necessarily civil liberties. Information can be shared in a manner consistent with the protection of civil liberties. It is the nature and techniques of the surveillance that matters. Who performs the surveillance may also matter, but the conditions of the performance are of the most critical importance.[72] Moreover, it is also possible that the participation of multiple government agencies in the same intelligence operation, far from threatening civil liberties, might serve instead to check potential overreaching by individuals within one of the agencies.[73] In the end, the focus of attention should be principally on the techniques by which intelligence is gathered domestically and not on whether other members of the intelligence community are permitted to view the intelligence gathered as a result of those operations.

[72] If the CIA were to conduct domestic operations, or begin to task the FBI, then alarm we consider overly-cautious here might be demanded. Just as restrictions on military assistance to domestic authorities has continuing validity (and contains reasonable exceptions) so may restrictions on the domestic operation of the CIA. *See* 18 U.S.C. 1385, commonly called the *Posse Comitatus* Act.

[73] The goals of Executive Order 12333, which provides guidelines for coordination among the different elements of the United States Intelligence community, include "fostering analytical competition among appropriate elements of the Intelligence Community" and "ensuring that appropriate mechanisms for competitive analysis are developed so that diverse points of view are considered fully and differences of judgment within the Intelligence Community are brought to the attention of national policymakers." Executive Order 12333, *supra* note 18, at ''1.1(a), 1.5(k).