Order Code RL33873

CRS Report for Congress

Sharing Law Enforcement and Intelligence Information: The Congressional Role

February 13, 2007

Richard A. Best Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Prepared for Members and
Committees of Congress

Sharing Law Enforcement and Intelligence Information: the Congressional Role

Summary

Almost all assessments of the attacks of September 11, 2001, have concluded that U.S. intelligence and law enforcement agencies had failed to share information that might have provided advance warning of the plot. This realization led Congress to approve provisions in the USA PATRIOT Act (P.L. 107-56) and subsequent legislation that removed barriers to information sharing between intelligence and law enforcement agencies, and mandated exchanges of information relating to terrorist threats. Most experts agreed that statutory changes, albeit difficult to enact, were essential to change the approaches taken by executive branch agencies.

The barriers that existed prior to September 2001 had a long history based on a determination to prevent government spying on U.S. persons. This had led to the establishment of high statutory barriers to the sharing of law enforcement and intelligence information. The statutes laid the foundation of the so-called "wall" between intelligence and law enforcement that was buttressed by regulations, Justice Department policies, and guidance from the judicial branch.

Despite the widespread acceptance of a barrier between law enforcement and intelligence, by the early 1990s it had become apparent to some that the two communities could mutually support efforts to combat international criminal activities including narcotics smuggling. Later in the decade dangerous threats to the U.S. posed by international terrorists came into sharper focus. Nevertheless, efforts to adjust laws, regulations, and practices did not succeed, drawing strong opposition from civil libertarians. Only the tragedy of the 9/11 attacks overcame earlier concerns and led Congress and the executive branch to remove most statutory barriers to information sharing.

Laws and regulations have changed significantly since September 2001 and an Information Sharing Executive (ISE) has been established within the Office of the Director of National Intelligence to design and implement information sharing procedures. It is clear, however, that sustaining the exchange of law enforcement and intelligence information remains a challenge. In particular, there is continued concern about sharing of information that might in some way jeopardize the rights of free speech or association of U.S. persons. This opposition has contributed to the difficulty Congress has had in addressing legislation in this area and can be expected to continue. Some argue that, given the extent of legislation enacted in recent years, extensive oversight of information sharing efforts may be an appropriate way to ensure that the balance between ensuring domestic security and protecting civil liberties can be maintained.

This report will be updated as additional information becomes available.

Contents

The Legacy of FISA 2

Recognizing the Need to Share Information 3

Initial Efforts to Legislate 6

After 9/11, Congress Tears Down the Wall 10

Conclusion 14

Sharing Law Enforcement and Intelligence Information: the Congressional Role

Introduction

The failure of the U.S. Intelligence Community to provide better warning of the September 11, 2001, attacks has been widely attributed to the existence of "walls" between intelligence and law enforcement agencies. The walls arguably kept analysts from talking to each other and from sharing pieces of information that, if they had been viewed in close relationship, might have yielded a coherent picture of the emerging plot. This theory cannot of course be fully proven — the overall plot might not have been discerned even if the best analysts had had access to all available information in every agency. Nevertheless, the fact that available data had not in fact been shared focused public and congressional attention on the real or perceived walls that inhibited the exchange of information among agencies.

A consensus emerged that the walls should be torn down. In December 2002, the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, established by the two congressional intelligence committees, made a factual finding that the "important point is that the Intelligence Community, for a variety of reasons, did not bring together and fully appreciate a range of information that could have greatly enhanced its chances of uncovering and preventing Usama Bin Ladin's plan to attack the United States on September 11, 2001."[1] The Inquiry also made a systemic finding that:

> Within the Intelligence Community, agencies did not adequately share relevant counterterrorism information, prior to September 11. This breakdown in communications was the result of a number of factors, including differences in the agencies' missions, legal authorities and cultures. Information was not sufficiently shared, not only between different Intelligence Community agencies, but also within individual agencies, and between the intelligence and law enforcement agencies.[2]

---

[1] U.S. Congress, 107th Congress, Senate, Select Committee on Intelligence, and House of Representatives, Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, Report, S.Rept. 107-351, H.Rept. 107-792 [Hereafter: *Joint Inquiry Report]*, December 2002, p. 33.

[2] Ibid., p. xvii. Intelligence agencies focus on concerns outside U.S. territory (and are sometimes known as "foreign intelligence" agencies). They include the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Reconnaissance Office (NRO), the National Geospatial-Intelligence Agency (NGA), the Bureau of Intelligence and Research of the State Department, the intelligence components of the military services and the Department of Homeland Security.

(continued...)

Similar conclusions were reached in July 2004 by the 9/11 Commission (the National Commission on Terrorist Attacks Upon the United States) carefully documented the failures of pre-9/11 information sharing among agencies and within different offices of the Justice Department and recommended a number of initiatives to encourage unity of effort in sharing information.[3]

The Legacy of FISA

The failure to share information prior to 9/11 had not occurred by happenstance. Law enforcement and intelligence information was not routinely shared and collectors and analysts were walled off from one another through a complex arrangement of constitutional principles, statutes, policies, and practices. These regulations had their origin in longstanding divisions of labor that reached back far into pre-World War II practices and in the provision of the National Security Act of 1947 requiring that the Central Intelligence Agency (CIA) "have no police, subpoena, or law enforcement powers or internal security functions."[4] The regulations were significantly strengthened in the 1970s when, in reaction to domestic intelligence gathering activities during the Vietnam War era, Congress undertook extensive investigations of intelligence activities and enacted legislation regulating domestic surveillance activities. Ultimately, in response to recommendations derived from this investigation, in 1978 Congress passed and President Jimmy Carter signed the Foreign Intelligence Surveillance Act (FISA), P.L. 95-511[5]. FISA provides a statutory framework for electronic surveillance in foreign intelligence investigations while electronic surveillance in criminal investigations continues to be governed by Title III of the Omnibus Crime Control Act of 1968 (usually referred to as Title III).[6]

---

[2] (...continued)
Law enforcement agencies include the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration, the Secret Service, and the Customs Service. The FBI is considered both a foreign intelligence agency and a law enforcement agency; this is also the case with the Coast Guard.

[3] U.S., National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington: Government Printing Office, 2004); see pp. 416-419.

[4] 50 U.S.C. 403-3(d)(1); on FISA generally, see CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*, by Elizabeth B. Bazan.

[5] In 1994 FISA was modified to include physical searches (section 807 of the Intelligence Authorization Act for FY1995, P.L. 103-359).

[6] Title III prohibits all interception of wire or electronic communications unless that interception falls within one of the exceptions to Title III; electronic surveillance under FISA is one of the exceptions (18 U.S.C. 2511(2)(f). It is to be noted that "foreign intelligence" may not involve actual or potential violations of U.S. laws, *e.g.* intelligence could be acquired, in the U.S., regarding a plot involving parties outside the U.S. that would not involve activities prohibited by U.S. law. Such intelligence could be of great interest to national policymakers but there would be no justification for relying on Title III surveillance authorities in trying to obtain it. As will be noted below, there is, however, a significant potential for overlap when intelligence provides evidence of activities that are
(continued...)

The implementation of FISA came to have an important influence on the relationship between law enforcement and intelligence.

FISA required that "the purpose" of domestic electronic surveillance (or a physical search) had to be the gathering of foreign intelligence information.[7] FISA permitted the dissemination to the law enforcement community of information relating to criminal activity incidentally acquired during a FISA electronic surveillance or physical search. When such dissemination was challenged by defense attorneys as running afoul of the Fourth Amendment,[8] a number of federal courts of appeals had upheld the government's contention in several cases that the "primary purpose" of an electronic surveillance or physical search had been the collection of foreign intelligence information. Thus, this use of FISA was held to be not inconsistent with Fourth Amendment requirements for criminal cases.[9]

Before 9/11 a considerable body of government practice and Justice Department policy increasingly reflected an understanding that adhering to the primary purpose standard effectively precluded Fourth Amendment challenges. The concern was to avoid letting aggressive criminal investigators obtain FISA court orders when they were interested in obtaining evidence of criminal activities. There was a pervasive concern within the Justice Department that a court in a criminal trial would suppress information obtained through a FISA investigation on the grounds that it was primarily being used, not to collect foreign intelligence, but to gather criminal evidence or even that FISA itself would be overturned. In practice, information collected by intelligence agencies (including the parts of the Federal Bureau of Investigation (FBI) dealing with counterterrorism and counterintelligence) was kept apart from information collected for the use of prosecutors.

Recognizing the Need to Share Information

FISA's requirements appear not to have posed major problems until the mid-1990s,[10] but law enforcement and intelligence agencies tended to function in separate

---

[6] (...continued)
illegal under U.S. law.

[7] 50 U.S.C. 1804(a)(7)(B), 50 U.S.C. 1823(a)(7)(B). Sec. 218 of the USA PATRIOT Act (P.L. 107-56) had amended these sections to replace "the purpose" with "a significant purpose."

[8] The Fourth Amendment to the Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[9] A detailed assessment of the various judicial views and rulings on this question lies beyond the scope of this Report; see, however, David S. Kris, "The Rise and Fall of the FISA Wall," *Stanford Law and Policy Review*, Spring 2006, pp. 487-529.

[10] See Diane Carraway Piette and Jesselyn Radack, "Piercing the 'Historical Mists': the (continued...)

worlds. Concern about these divisions did exist and there had been major initiatives largely as a result of concerns about the development of barriers between law enforcement and intelligence agencies in the aftermath of the controversy surrounding the illegal activities of the Banca Nazionale del Lavoro (BNL) and the Bank of Credit and Commerce International (BCCI) in the early 1990s. The controversy involved complex banking fraud and other criminal activities undertaken by the two foreign banks. Congressional investigators developed information that the CIA had obtained information indicating suspicious activities by the two banks that had not been passed to prosecutors in large measure because channels of communications had not been established between intelligence and law enforcement agencies. The Senate Intelligence Committee investigators concluded that:

> The fundamental policy governing the relationship between law enforcement and intelligence needs to be addressed by the Attorney General and the DCI [Director of Central Intelligence], in conjunction with the congressional oversight committees. Confusion is apparent on both sides as to what the proper role (and authority) of intelligence agencies is in circumstances like those presented in the BNL case.[11]

The reaction to the BNL/BCCI affairs reflected a shift away from emphasis on a strict separation of law enforcement and intelligence efforts to an appreciation by Congress of the need for closer cooperation. As a result of congressional concerns, the DCI and the Attorney General directed that a review of the intelligence-law enforcement relationship be conducted. The review, undertaken by a group of senior executive branch officials known as the Joint Task Force on Intelligence and Law Enforcement, submitted a report in August 1994. The Task Force described the failure by intelligence and law enforcement agencies to make use of all available information on the activities of the two foreign banks. It called for a number of bureaucratic mechanisms to ensure greater information exchanges in the future, but argued that no statutory changes were called for:

> What is required is not new legislation radically altering the relationship [between intelligence and law enforcement agencies], but rather a different approach to the existing relationship — one that is more interactive on a number of fronts, yet maintains the important distinctions between these two communities based on law, culture, and mission.[12]

---

[10] (...continued)
People and Events Behind the Passage of FISA and the Creation of the 'Wall,'" *Stanford Law and Policy Review*, Spring 2006, p. 461.

[11] U.S. Congress, 103d Congress, 1st session, Senate, Select Committee on Intelligence, *The Intelligence Community's Involvement in the Banca Nazionale del Lavoro (BNL) Affair*, S. Prt. 103-12, February 1993, p. 27.

[12] U.S., Joint Task Force on Intelligence and Law Enforcement, *Report to the Attorney General and Director of Central Intelligence*, August, 1994, p. 4. The absence of a need for legislation was also the position of the then-DCI James Woolsey: "Rather, we can accomplish our goal of enhanced cooperation through a series of initiatives — such as joint training of law enforcement and intelligence officers." Address by R. James Woolsey, Director of Central Intelligence, before the American Bar Association, Washington, DC, (continued...)

The Joint Task Force Report led to the establishment of a series of interagency coordinative mechanisms — the Intelligence-Law Enforcement Policy Board, the Joint Intelligence-Law Enforcement Working Group (JICLE) — at various levels to encourage information exchanges and resolve difficulties.[13] Although the Task Force provided a perceptive analysis of the difficulties that then existed and officials assigned to the resultant interagency bodies worked diligently at overcoming obstacles, progress was limited.[14]

By the 1990s, the threat of new forms of international terrorism was becoming apparent. Middle Eastern terrorists were operating against U.S. forces overseas and, occasionally, within the U.S. (as in the 1993 World Trade Center attacks). Observers believed that both intelligence and law enforcement agencies were collecting relevant information on international terrorism. Members of Congress began to seek administrative and statutory changes that could facilitate information sharing in this area.

Pursuant to P.L. 105-277, a supplemental appropriations act passed in 1998, the National Commission on Terrorism, headed by former Ambassador L. Paul Bremer, was established to review the laws, regulations, directives, policies and practices for preventing and punishing international terrorism. The Bremer Commission's June 2000 report highlighted concerns about the inadequate sharing of terrorism-related information. It recommended the elimination of barriers to the aggressive collection of information on terrorists and suggested that the FBI suffered from bureaucratic and cultural obstacles to gathering terrorism information. It found that the "Department of Justice applies the statute governing electronic surveillance and physical searches of international terrorists in a cumbersome and overly cautious manner."[15] Although it noted that the FISA application process had been recently streamlined, it recommended that the Justice Department's Office of Intelligence Policy Review

---

[12] (...continued)
April 29, 1994. In 2001, however, Woolsey would write in regard to the 1993 World Trade Center bombing, "No one other than the prosecutors, the Clinton Justice Department, and the FBI had access to the materials surrounding the case until they were presented in court, because they were virtually all obtained by a federal grand jury and hence kept not only from the public but from the rest of the government under the extreme secrecy requirements of Rule 6(e) of the Federal Rules of Criminal Procedure." R. James Woolsey, "Blood Baath: the Iraq Connection," *New Republic*, September 24, 2001, p. 21. Rule 6(e) established requirements for the secrecy of grand jury proceedings.

[13] See CRS Report RL30252, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, by Richard A. Best Jr.

[14] A key factor appears to have been the potential that litigation over important espionage cases could jeopardize existing practices; see, for instance, the testimony of John Gannon, former head of the National Intelligence Council and other senior government positions, to the Senate Judiciary Committee, May 2, 2006; Gannon claimed that the "early post-war determination to share information and push the 'wall' on information sharing between intelligence and law enforcement was set back by the sensational Ames, Nicholson, and Hanson espionage cases."

[15] U.S., National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, June 2000, p. 10.

(OIPR) should not require the inclusion of information in excess of that which was actually mandated by FISA. It also recommended that OIPR be substantially expanded and that it be directed to cooperate with the FBI.[16]

The Commission further concluded:

> Law enforcement agencies are traditionally reluctant to share information outside of their circles so as not to jeopardize any potential prosecution. The FBI does promptly share information warning about specific terrorist threats with the CIA and other agencies. But the FBI is far less likely to disseminate terrorist information that may not relate to an immediate threat even though this could be of immense long-term or cumulative value to the intelligence community. . . . Moreover, certain laws limit the sharing of law enforcement information, such as grand jury or criminal wiretap information, with the intelligence community. These laws are subject to different interpretations, so that in some cases it is unclear whether the restrictions apply."[17]

The Commission did not indicate a need for immediate statutory changes, but recommended that the "Attorney General should clarify what information can be shared and direct maximum dissemination of terrorist-related information to policymakers and intelligence analysts consistent with the law."[18]

Initial Efforts to Legislate

Members of Congress did propose various approaches to address the lack of information sharing. S. 2089 as introduced in February 2000 by Senator Specter, would have required that the Attorney General prescribe in regulations the circumstances under which information acquired pursuant to FISA "shall be disclosed for law enforcement purposes." The bill would also have required two reports addressing issues of information sharing. First, it would have tasked the Director of the FBI to submit a report on "the feasibility of establishing within the Bureau a comprehensive intelligence reporting function having the responsibility for disseminating among the elements of the intelligence community information collected and assembled by the Bureau on international terrorism and other national security matters." Secondly, the bill would have required the President to submit a report on the legal authorities that govern the sharing of criminal wiretap information with intelligence agencies and with recommendations to improve the capability of the Justice Department to share "foreign intelligence information or counterintelligence information with elements of the United States intelligence community on matters such as counterterrorism."

In its report on the bill, the Senate Intelligence Committee argued:

---

[16] Ibid., p. 12.

[17] Ibid., pp. 15-16.

[18] Ibid, p.16.

> For the intelligence mission of the United States to be successful, there must be a cooperative and concerted effort among intelligence agencies. Any information collected by one agency under foreign intelligence authorities that could assist another agency in executing its lawful mission should be shared fully and promptly....
>
> The Committee has been briefed on the recent efforts by the Federal Bureau of Investigation and the Central Intelligence Agency to enhance their ability to share valuable information collected under FISA orders. The Committee commends these efforts and expects them to continue and to be broadened to include all areas of the foreign intelligence mission.[19]

As reported to the Senate in July 2000, S. 2089 was modified to include only a request for reports from the Attorney General on mechanisms for determinations of disclosure of FISA-derived information for law enforcement purposes and on actions taken by the Department of Justice (DOJ) to coordinate the dissemination of intelligence information within DOJ.

Congressional concern about the growing threat of terrorism was also demonstrated in S. 3205, introduced in October 2000 and known as the Kyl-Feinstein Counterterrorism Act of 2000, which was based directly on recommendations of the Bremer Commission that had been released in August. The bill took notice of the attack on the U.S.S. *Cole*, which had occurred on October 12, 2000, and aimed to discourage financial support of terrorist organizations. This bill also addressed information sharing issues; section 9 would have required a report on the feasibility of assigning the FBI responsibility for disseminating among the elements of the Intelligence Community information collected and assembled by the FBI on international terrorism and other national security matters. Section 10 of the bill would have required a report on the legal authorities that govern the sharing of criminal wiretap information with various law enforcement agencies and intelligence agencies and "recommendations, if any," for legislative language that would improve the Justice Department's capabilities to share information on matters such as counterterrorism with intelligence agencies "with elements of the United States intelligence community on matters such as counterterrorism."

Consideration of the legislation reflected many of the same privacy and civil liberties concerns that had influenced existing procedures in the Justice Department. Criticisms of the approach taken by the legislation were voiced by some civil libertarians. One group opposed the sharing of information obtained by electronic surveillance conducted under Title III authorities with intelligence agencies. Such an effort, it was argued, "breaches the well-established and constitutionally vital line between law enforcement and intelligence activities."[20] Concern was also expressed about the potential use of such information by the CIA and other intelligence

---

[19] U.S. Congress, 106th Congress, 2d session, Senate, Select Committee on Intelligence, *The Counterintelligence Reform Act of 2000*, S.Rept. 106-352, July 20, 2000, p. 6.

[20] Letter from Laura W. Murphy, Director, American Civil Liberties Union, Washington National Office, James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology, and Kate Martin, Executive Director, Center for National Security Studies, reprinted in *Congressional Record*, October 26, 2000, p. S11118.

agencies: "The secretive data gathering, storage and retention practices of the intelligence agencies are appropriate only when conducted overseas for national defense and foreign policy purposes and only when directed against people who are not U.S. citizens or permanent residents."[21] Further concern was directed at the potential use of information gathered under counterintelligence authorities (presumably FISA) in criminal proceedings:

> Since the period of ... the Church committee, it has been recognized that the rights of Americans are better protected (and the FBI may be more effective) when international terrorism and national security investigations are conducted under the rules for criminal investigations.[22]

Such views reflected a continuing distrust of intelligence agencies and a fear that past practices might be revived. In floor debate, Senator Leahy noted that initial drafts of S. 3205 had posed "serious constitutional problems and risks to important civil liberties we hold dear." After modifications, however, "no longer does the bill require a change in the wiretap statute allowing the permissive disclosure of information obtained in a Title III wiretap to the intelligence agencies."[23]

The Clinton Administration Justice Department took a different approach, arguing that then-current statutes and regulations provided law enforcement agencies with "authority under current law to share Title III information regarding terrorism with intelligence agencies when the information is of over-riding importance to the national security." Any change "must accommodate legal constraints such as Criminal Rule 6(e) and the need to protect equities relating to ongoing criminal investigations."[24] Accordingly, the Justice Department specifically opposed the provision in the bill that would permit the sharing of foreign intelligence or counterintelligence information collected under Title III by investigative or law enforcement officer with intelligence agencies.[25]

The Kyl-Feinstein bill would not have changed statutory language, but only asked for reports on the issue of information. Even so, according to Senator Leahy,

---

[21] Ibid.

[22] Ibid., p. S11119.

[23] *Congressional Record*, November 14, 2000, p. S11540. Almost a year later during consideration of the USA PATRIOT Act, Senator Leahy would note that the Justice Department had opposed the original Kyl legislation because it might have opened sensitive materials to the discovery process and it raised issues about sharing information about U.S. persons. *Congressional Record*, October 25, 2001, p. S11001.

[24] Letter from Robert Raben, Assistant Attorney General, Department of Justice, reprinted in *Congressional Record*, October 26, 2000, pp. S11119. The letter did not elaborate on how Rule 6(e) and the need to protect equities could be balanced against the need to share information. Apparently, precise details of a planned assassination plot would meet the "overriding importance" standard, but Raben gave no recognition that intelligence agencies should have access to ambiguous data that might yield evidence of a plot only when combined with other information; in other words, dots that are innocuous in themselves but which, when connected to other information, reveal a dangerous threat.

[25] Ibid., p. S11119.

the initial proposal to mandate such changes "prompted a firestorm of controversy from civil liberties and human rights organizations, as well as the Department of Justice."[26] Even though the House took no action on this bill, passage of the legislation by the Senate reflected concerns at the end of 2000 regarding the possible need to adjust information sharing mechanisms, coupled with a determination to move cautiously before implementing changes that could affect civil liberties. Ultimately, the legislation was adopted by the Senate on November 14, 2000, but it was not sent to the House before the adjournment of the 106th Congress.

The FY2001 Intelligence Authorization Act, P.L. 106-567, signed on December 27, 2000, reflected the concerns that had inspired both S. 2089 and S. 3205. It included a requirement for a report from the Attorney General on "the authorities and procedures utilized by the Department of Justice for determining whether or not to disclose information acquired under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for law enforcement purposes."[27] This Act also formalized procedures for authorizing FISA surveillance, expanded grounds for establishing probable cause, established new procedures for physical searches within FISA, and specified mechanisms to facilitate the use of intelligence in counterintelligence investigations. It provided increased funding for OIPR subsequent to the submission of a report indicating efforts taken to streamline and improve the FISA application process. It included a provision (in section 606) derived from S. 2089 requiring a report from the Attorney General on actions taken to "coordinate the dissemination of intelligence information within the appropriate components of the [Justice] Department and the formulation of policy on national security issues." It did not, however, address the question of making information from law enforcement sources available to the Intelligence Community.

Clearly, the problems created by the existence of the "wall" had not been unrecognized prior to 9/11. The Justice Department's opposition in 2000 to legislative proposals to remove barriers has been noted. On the other hand, some argue that the primary factor in preventing statutory changes was, as one observer has claimed, that "in most instances both the Department of Justice and The White House turned down the requests because it was firmly believed by senior members of the Executive Branch that the United States Congress would not allow the IC [Intelligence Community] to have broader surveillance powers."[28] This view would

---

[26] *Congressional Record*, November 14, 2000, p. S11540; Leahy himself, however, had earlier that year indicated support for legislation that would promote information sharing and consultation between intelligence agencies in regard to counterintelligence. "In an area of such national importance, it is critical that our law enforcement and intelligence agencies work together as efficiently and cooperatively as possible." Prepared Statement of Hon. Patrick Leahy printed in U.S. Congress, 106th Congress, 2d session, Senate, Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, *Counterintelligence Reform Act of 2000,* S.Hrg. 106-993, March 7, 2000, p. 12.

[27] Section 604(b), P.L. 106-567.

[28] Robert M. Blitzer (a former FBI official), "Domestic Intelligence Challenges in the 21st Century," (Arlington, VA: Lexington Institute, 2002), p. 10; available at [http://www.lexingtoninstitute.org/docs/497.pdf].

be expressed by former Attorney General William Barr in testimony to the 9/11 Commission:

> For three decades leading up to 9/11, Congress was at the fore of a steady campaign to curtail the Bureau's domestic intelligence activities and impose on all its activities the standards and process of the criminal justice system. These concerns made it extremely difficult for the Bureau to pursue domestic security matters outside the strictures of the criminal justice process. Prohibitions on sharing grand jury information with intelligence agencies and with using intelligence information in criminal investigations created a 'wall of separation.'[29]

It is clear in retrospect that there were those in both the Executive Branch and Congress who realized the need to lower barriers to sharing law enforcement and intelligence information, but their views did not, prior to 9/11, reflect a consensus in either branch. Those opposed to greater information sharing did so in large measure because of their awareness of the past history of domestic surveillance and a distrust of intelligence organizations. The result was a number of very tentative steps that, in the event, proved wholly inadequate to task of gathering information about al Qaeda's plot. The FY2001 Intelligence Authorization Act included some minimalist provisions, but the wall was left in place. Neither the Clinton Administration or the Bush Administration, in the first eight months of 2001, sought to amend the relevant laws.[30] The problem was recognized but proposed solutions faced strong opposition.

After 9/11, Congress Tears Down the Wall

The attacks of September 11, 2001, destroyed the World Trade Center and a portion of the Pentagon; they also demolished the wall between U.S. law enforcement and intelligence. After 9/11, it was almost immediately accepted that counterterrorism would have to involve all parts of the U.S. Government, including law enforcement agencies and the Intelligence Community. It was agreed that the counterterrorism effort must be based on sharing information from whatever source. The problem for both Congress and the executive branch was to establish appropriate mechanisms for information sharing with adequate safeguards for using the information in future criminal trials.

Congress immediately set about to consider the most appropriate legislative response that could be quickly enacted. Former Attorney General John Ashcroft

---

[29] Statement of William P. Barr to the 9/11 Commission, December 8, 2003; available at [http://www.9-11commission.gov/hearings/hearing6/witness_barr.htm].

[30] The incoming Bush Administration was reviewing procedures relating to the wall, but as late as August 2001, Larry D. Thompson, the Deputy Attorney General, reiterated that departmental guidelines regarding the wall were still in effect; Larry D. Thompson Memorandum to Criminal Division, Office of Intelligence Policy and Review, and FBI, August 6, 2001 available at [http://www.cnss.org/9.11commissionintelligence.htm]; see also, John Ashcroft, *Never Again: Securing America and Restoring Justice* (New York: Center Street, 2006), p. 147; Thomas H. Kean and Lee H. Hamilton, *Without Precedent: the Inside Story of the 9/11 Commission* (New York: Knopf, 2006), p. 195.

writes, "The 9/11 attacks occurred on a Tuesday. By Saturday, we had a full-blown legislative proposal. Part of the reasons we were able to move so quickly was that a number of the provisions had been proposed to Congress in 1996, and Congress had rejected them."[31] Attention focused on various proposals and recommendations of commissions that had looked at international terrorism and related issues and to earlier legislative proposals that had not been adopted.[32] A wide number of proposals came together as the USA PATRIOT Act (P.L. 107-56) that would be debated in the final weeks of September and early October 2001.[33] The USA PATRIOT Act changed the requirement that "the purpose" of a FISA surveillance be to collect foreign intelligence information, to require that collecting such information be "a significant purpose" of FISA electronic surveillance or physical search. This provided latitude to use FISA authority for electronic surveillance or physical searches where the primary purpose was criminal investigation, as long as a significant foreign intelligence purpose was also present.

The USA PATRIOT Act also addressed concerns about sharing intelligence and law enforcement information. Although a discussion of all the complex provisions that were included in the USA PATRIOT Act lies beyond the scope of this Report,[34] several provisions address the sharing of law enforcement and intelligence information. Section 203 of the Act removed some of the restrictions on federal government attorneys sharing grand jury information. Subsection 203(a) authorized federal government attorneys to share matters occurring before the grand jury involving foreign intelligence, counterintelligence, or foreign intelligence information with a federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist that official in the performance of his or her duties. Subsection (a) authorized the sharing of grand jury information "when the matters involve foreign intelligence or counterintelligence."[35]

Subsection 203(b) permitted investigative and law enforcement officers and Government attorneys to share information acquired under or derived from the

---

[31] Ashcroft, *Never Again*, p. 154.

[32] One skeptical observer noted that the "great majority of the new surveillance provisions had been discussed within the executive branch or Congress in previous years and had not been adopted. After the September 11 attacks, professional staff in the agencies simply went into their files and pulled out provisions they had been advocating previously. In the super-charged climate of the fall of 2001 many of these provisions received remarkably little scrutiny or debate." Peter P. Swire, "The System of Foreign Intelligence Surveillance Law," *George Washington Law Review*, August 2004, p. 1349.

[33] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 (P.L. 107-56; signed October 26, 2001). The legislation was adopted by a 357-66 vote in the House and a 98-1 vote in the Senate.

[34] See CRS Report RL31377, *The USA PATRIOT Act: A Legal Analysis*, by Charles Doyle.

[35] Section 203(a)(1) provides that any Federal official to whom such information is made available may use it only in the conduct of that person's official duties. Further: "Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made."

interception of a wire, oral, or electronic communication under Title III with any other federal law enforcement, intelligence, protective, immigration, national defense or national security official for use in his or her official duties to the extent that the contents of that communication include foreign intelligence or counterintelligence information.

Subsection (c) provides authority for the Attorney General to establish implementing procedures.

Subsection 203(d) permitted the disclosure of foreign intelligence, counterintelligence, or foreign intelligence information obtained as part of a federal criminal investigation, notwithstanding any other provision of law, to any federal law enforcement, intelligence, protective, immigrations, national defense, or national security official in order to assist that official in carrying out his or her official duties, subject to any limitations on the unauthorized disclosure of that information.

Section 504 permitted federal officers conducting electronic surveillance or physical searches under FISA to consult with federal law enforcement officers or state or local law enforcement personnel to coordinate against actual or potential attacks or other grave hostile acts of a foreign power or its agent; sabotage or international terrorism by a foreign power or its agent, or clandestine intelligence activities by an intelligence service or network of a foreign power or its agent.

Section 905 requires the Attorney General or heads of other Federal agencies with law enforcement responsibilities to disclose expeditiously to the DCI (later replaced by the Director of National Intelligence (DNI)), under relevant guidelines, foreign intelligence acquired in the course of a criminal investigation. Exceptions could be made where the disclosure of such foreign intelligence would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests. In addition, Section 905 required the Attorney General, in consultation with the DCI (now the DNI), to develop procedures to give the Director timely notice of the Attorney General's decision to begin or decline to begin a criminal investigation based on information from an element of the intelligence community regarding possible criminal activity of a foreign intelligence source or potential source.[36]

---

[36] The Act provided that some, but not all, of its provisions would expire (or "sunset") at the end of 2005, giving Congress the opportunity to assess their effects in the intervening months. Subsections 203(b) and 203(d) (but not (a) and (c)) were among those that were scheduled to sunset; section 905 was not scheduled to sunset. As noted by Charles Doyle, CRS Report RL32186, *USA PATRIOT Act Sunset Provisions That Were to Expire on December 31, 2005*, these provisions are similar to and may duplicate other statutory provisions in the USA PATRIOT Act and other legislation that were not scheduled to sunset; the legal issue regarding the extent to which these provisions are in fact duplicative lies beyond the scope of this Report. In any event, P.L.109-177, signed on March 9, 2006, made subsections 203(b), 203(d) and 905 permanent. See also CRS Report RL33332, *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis*, by Brian T. Yeh and Charles Doyle.

The provisions included in the USA PATRIOT Act and DOJ's effort to implement them were far-reaching and to some extent were not welcomed by the FISA Court. In particular, the FISA Court in *In re all Matters Submitted to the Foreign Intelligence Court* found that proposed 2002 procedures issued by the Attorney General "eliminate[d] the bright line in the 1995 procedures prohibiting direction and control by prosecutors on which the Court has relied to moderate the broad acquisition[,] retention, and dissemination of FISA information in overlapping intelligence and criminal investigations."[37] The FISA Court thus attempted to "reinstate the bright line used in the 1995 procedures, on which the Court has relied."[38]

Concerned that its proposed procedures were rejected, the Justice Department appealed the Foreign Intelligence Surveillance Court's granting of a request modified in accordance with its earlier ruling in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*. The appeal went to the Foreign Intelligence Surveillance Court of Review and was the first appeal to that court. In a sweeping decision, the Court of Review overruled the limitations imposed by the FISA Court, along with a considerable amount of customary FISA practice. The Court of Review expressed concern that the FISA Court had overstepped its role by prescribing the internal procedures for handling surveillances within the Justice Department. The Court of Review maintained that the FISA Court "determined an investigation became primarily criminal when the Criminal Division played a lead role. This approach has led, over time, to the quite intrusive organizational and personnel tasking the FISA [C]ourt adopted. Putting aside the impropriety of an Article III court imposing such organizational strictures ... [the wall] was unstable because it generates dangerous confusion and creates perverse organizational incentives."[39] The Court of Review thereby gave the final blow to the legal structure supporting the wall between law enforcement and intelligence information.

Implementation of the information-sharing provisions of the USA PATRIOT Act and other legislation is underway. The Homeland Security Act of 2002 (P.L. 107-296) and the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required that procedures be established under which federal agencies can share intelligence and law enforcement information about international terrorism. The Intelligence Reform Act mandated the creation of an Information Sharing Environment (ISE) that combines policies, procedures, and technologies to link information collections and users. In November 2006 the Administration released a lengthy implementation plan for the ISE. The plan sets forth procedures for sharing information among agencies at federal, state, and local levels and seeks to promote a culture of information sharing. It also provides procedures for protecting

---

[37] In re all matters submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp.2d, pp. 621-622 (May 17, 2002).

[38] Ibid., p. 625.

[39] In re Sealed Case, 310 F.3d, p. 743 (November 18, 2002).

information privacy and civil liberties.[40] Congress may choose to review the implementation of the ISE during coming months.

Conclusion

A fundamental issue that faces both Congress and the U.S. public remains the need to balance the advantages to be gained by sharing information from all sources with the possibility that the availability of data accumulations could be used to undermine lawful political or religious activities. An unstable balance between these two separate goals — often portrayed as competing — greatly complicated the counterterrorism and counterintelligence effort prior to 9/11. The fact that public opinion appeared deeply ambivalent made procedural changes difficult and contributed to the luxuriant growth of complex regulations adopted by DOJ and endorsed by the FISA Court. After 9/11, public opinion shifted dramatically, resulting in the rapid passage of the USA PATRIOT Act and other legislation. The need to encourage the sharing of information and the connection of dots is now unquestioned, but there are lingering concerns about the risks that widespread information sharing may jeopardize civil liberties. Congress will undoubtedly seek to determine whether the new statutes, regulations, and procedures that have been adopted will prove both effective and sensitive to individual rights.

The importance of sharing intelligence and law enforcement information is not limited to issues relating to international terrorism but extends to banking fraud, narcotics smuggling, and a variety of international concerns. Narcotics smuggling, for instance, can be addressed by encouraging other countries to halt the cultivation of opium poppies or coca, as well as by law enforcement in the U.S. Terrorism, of course, is uniquely threatening and in combating terrorists more vigorous non-law enforcement approaches are considered more legitimate than is the case with drug smugglers or embezzlers. What is advantageous in all cases is assembling the full range of information about the activity and subjecting it to rigorous analysis.

There is, however, the possibility that the current consensus may unravel. The political controversy surrounding NSA's electronic surveillance efforts and other data mining programs may come to focus on the sharing of information that some argue was not lawfully obtained, and this concern could lead to efforts to restrict information sharing across the boards. There is also a possibility that the use of information obtained by surveillance in accordance with FISA might ultimately not be allowed in court cases out of concern that the Fourth Amendment has been

---

[40] The implementation plan is available at [http://www.ise.gov/docs/ISE-impplan-200611.pdf]. For additional background see U.S. Government Accountability Office, *Information Sharing: the Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385, March 17, 2006. Many of the initiatives in regard to the ISE have been widely criticized; see Ellen Nakashima, "Civil Libertarians Protest Privacy Policy; New Guidelines Do Little to Protect Established Rights, White House Board Told," *Washington Post*, Dec. 6, 2006, p. A11.

bypassed.[41] Despite the widespread acceptance of the need for information sharing, concerns that sharing information could lead to governmental abuses persists across the political spectrum. These concerns are tenaciously held, and have in the past made legislating very controversial. There is no reason to believe that they will not resurface should the threat from international terrorism seem less menacing.

The potential threat to civil liberties does not, of course, represent the full extent of the issues raised by increased information sharing. Sharing sensitive information inevitably raises the danger that intelligence sources and methods may be compromised either accidentally or purposefully. For intelligence professionals, in particular, the danger to valuable sources that may have taken years to develop is a fundamental concern. Moreover, when a human source is compromised there is not only a danger to a particular individual, but also a potential loss of confidence in U.S. intelligence agencies by other actual or potential sources.

The role of Congress in dealing with information sharing issues is especially important. There are delicate questions of liberty and security involved and a sensitive balance is crucial. Air Force General Michael V. Hayden, who now serves as CIA Director, in the past argued that Members of Congress are in close touch with their constituents and "What I really need you to do is talk to your constituents and find out where the American people want that line between security and liberty to be."[42] Congress also can provide the ongoing oversight to ensure that the sorts of abuses that occurred in the 1960s and 1970s do not recur. Ultimately, an information sharing policy that is largely consistent with public opinion and is held to account by rigorous oversight should enhance the chances that the dots can be connected without jeopardizing the rights of Americans. Observers see a danger, however, that gridlock in both the Executive and Legislative Branches might inhibit the government's ability to find effective and sensible ways to acquire and analyze information on new threats to the national security.

---

[41] This possibility was even alluded to by the November 2002 Foreign Intelligence Court of Review that maintained that "...a FISA order may not be a 'warrant' contemplated by the Fourth Amendment. The government does not actually claim that it is, instead noting only that there is authority for the proposition that a FISA order is a warrant in the constitutional sense." The Court of Review added: "We do not decide the issue but note that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment." In re: Sealed Case, 310 F.3d, p. 742.

[42] Testimony of Lt. Gen. Michael V. Hayden, USAF, U.S. Congress, 107th Congress, Senate, Select Committee on Intelligence, and House of Representatives, Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, Hearings, Vol. II, October 1, 3, 8 and 17, 2002, S.Hrg. 107-1086, pp.801-802.