

**STATEMENT  
OF  
LARRY D. THOMPSON  
SENIOR FELLOW, THE BROOKINGS INSTITUTION  
WASHINGTON, DC**

**BEFORE  
THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

**AUGUST 11, 2004**

**9-11 COMMISSION FINDINGS:  
SUFFICIENCY OF TIME, ATTENTION, AND LEGAL AUTHORITY**

Thank you for asking me here today. I am pleased to have this opportunity to share with you my thoughts and observations of some of the issues under consideration by this distinguished Committee.

**Congress Must Address the Patriot Act Provisions that are Scheduled to Sunset on an Expedited Basis and in an Apolitical Manner**

In its report, the 9-11 Commission ("Commission") recognized the importance of both intelligence collection and information sharing in our country's efforts to prevent and disrupt terrorism. The Commission also recognized that the new authorities given federal law enforcement and intelligence agencies under the USA Patriot Act are beneficial to our country's antiterrorism efforts. The beneficial aspects of the Patriot Act as it relates to information sharing were also noted by the report to the Joint Inquiry of House and Senate Intelligence Committees ("Joint Inquiry").

Although the Commission observed that some of the Patriot Act's provisions will sunset or cease to be in effect on December 31, 2005, it did not set forth specific recommendations concerning the Act, except to note that the Act should be the subject of a "full and informed debate." The report

of the Joint Inquiry was more affirmative and recommended that certain information sharing provisions of the Patriot Act not sunset.

At least 16 provisions of the Patriot Act will sunset on December 31, 2005. It is critically important that Congress act now to undertake a reasoned, dispassionate, apolitical and informed analysis of these provisions which are so important to our antiterrorism efforts. We do not want to let these provisions expire and get caught flat-footed, as a nation, possibly compromising our ability to adequately secure the public safety.

I agree with the Commission when it noted that many of the Patriot Act's provisions are basically non-controversial. For example, many provisions simply update our surveillance laws to reflect technological developments in a digital age.

Unfortunately, much of the discussion and debate about the Patriot Act is at the extremes. Some view the authorities under the Act as unnecessarily authoritarian, while others view those who have concerns as uninformed and willing to unnecessarily sacrifice the country's safety. Much of the debate about the Patriot Act is shrill and ill-informed. In fact, some actions taken by the Executive Branch in our antiterrorism efforts that have been criticized, like the designation of enemy combatants, in fact are completely unrelated to the Act. We have got to do better.

When I served in government, I came to realize that our country's success in fighting the threat of terrorism would increasingly depend on public confidence that the government can ensure the fair and impartial administration of justice for all Americans while carrying out its essential national security and public safety efforts. This is why a balanced, apolitical and quick review of the sunset provisions is needed. I urge such a review, and as a former government official who experienced the utility of these new authorities, I urge their renewal.

It is absolutely clear that the authorities given federal law enforcement and intelligence agencies under the Patriot Act have enabled officials to “connect the dots” about the plans and activities of terrorists and terrorist supporters. For example, section 203 of the Patriot Act expressly empowers law enforcement officials to share criminal investigative information that contains foreign intelligence or counterintelligence, including grand jury and wiretap information, with intelligence, protective, immigration, national-defense, and national-security personnel. And section 905 of the Patriot Act requires that the Attorney General, subject to certain exceptions, disclose to the Director of Central Intelligence foreign intelligence acquired by the Department of Justice in the course of a criminal investigation.

During my tenure in government, the Department of Justice utilized these provisions of the Patriot Act on dozens of occasions to disclose vital information to the intelligence community. The U.S. Attorney’s Office for the Southern District of New York, for example, had accumulated extensive intelligence during its investigation and prosecution of numerous significant terrorism cases, such as the 1993 attack on the World Trade Center and the 2000 attack on the U.S.S. Cole, that it was finally able to share with intelligence agencies after the passage of the Patriot Act.

In addition to allowing law enforcement officials to provide valuable information to the intelligence community, the Patriot Act also has enhanced the flow of information from intelligence officials to the law enforcement community. In particular, section 218 of the Patriot Act allows information obtained by intelligence officials pursuant to the Foreign Intelligence Surveillance Act (FISA) to be shared more readily with law enforcement officials. Before the enactment of the Patriot Act, courts had ruled that surveillance under FISA could be utilized only when foreign intelligence was the “primary purpose” of a national security investigation. *See, e.g., United States v. Truong*, 629 F.2d 908 (4th Cir. 1980). This “primary purpose” standard, however, had the effect of

discouraging intelligence investigators from sharing information and coordinating with law enforcement officers. While intelligence officials could share information with prosecutors, the decision to do so always rested with national security personnel, even though law enforcement agents were in a better position to determine what evidence was pertinent to their criminal case. The old legal rules therefore discouraged coordination and created what the Foreign Intelligence Surveillance Court of Review called “perverse organizational incentives.” *In re Sealed Case*, 310 F.3d 717, 743 (FISCR 2002).

Section 218 of the Patriot Act, however, changed the law to clarify that FISA can be used whenever foreign intelligence is a “significant purpose” of a national security investigation, thus allowing for greater sharing and consultation between intelligence and law enforcement officials. In addition, section 504 of the Patriot Act specifically permits intelligence investigators to consult with federal law enforcement officers to coordinate efforts to investigate or protect against threats from foreign powers or agents.

Following the enactment of the Patriot Act, the Department of Justice took a number of steps to implement the aforementioned provisions and fully realize the potential of increased coordination and information sharing between intelligence officers and law enforcement officers. To begin with, the Department of Justice issued guidelines on March 6, 2002, that expressly authorized—and indeed required—coordination between intelligence and law enforcement. The Foreign Intelligence Surveillance Court (FISC) rejected these guidelines in part on May 17, 2002, and imposed additional restrictions on coordination between intelligence officials and law enforcement officials. These restrictions imposed by the FISC hampered valuable information sharing and coordination between intelligence officials and law enforcement officials, and were thankfully overturned when the Foreign

Intelligence Surveillance Court of Review approved the Department's guidelines in full on November 18, 2002.

Following the passage of the Patriot Act, the Attorney General also instructed all U.S. Attorneys to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. At the time that I left the Department, thousands of files already had been reviewed, and information from this review had been used to open numerous criminal investigations. And finally, the Attorney General directed every U.S. Attorney to develop a plan to monitor terrorism and intelligence investigations, and to ensure that information about terrorist threats was shared with other agencies and criminal charges were considered.

I have witnessed firsthand the critical importance of section 218 of the Patriot Act to winning the war against terrorism. Section 218 has enabled the federal government to disrupt terrorist plots and arrest and prosecute terrorists, thus saving American lives. But section 218, like at least 15 other provisions contained in the Patriot Act, is scheduled to sunset at the end of 2005. Allowing section 218 to expire would be a tragic mistake. While I wholeheartedly endorse renewing all sunsetted Patriot Act provisions, it would be difficult for me to overemphasize the importance of making section 218 permanent. Simply put, section 218 is critical to the federal government's ability to conduct the coordinated, integrated campaign necessary to win the war against terrorism. Without section 218, our ability to prevent future terrorist attacks by "connecting the dots" could be seriously compromised.

Interestingly, the FISA Court of Review noted that before the Patriot Act, there was never any real difference between a FISA order's "intelligence" and "criminal" purposes. According to the Court of Review, the Patriot Act, by purporting to loosen a "purpose" test that was incorrectly

assumed to exist, actually imposed a balancing test between “criminal” and “intelligence” purposes. Nevertheless, FISA law today, actually says what Congress intended for it to say after the passage of the Patriot Act and that is why it is critically important that Section 218 not sunset.

### **A Civil Liberties Concern and the National Counterterrorism Center**

The Commission in its report duly noted the concern of civil liberties in connection with these new authorities. I agree. I also agree with the Joint Inquiry that Congress continue its robust oversight of domestic law enforcement and intelligence authorities, including FISA and the Patriot Act. The Commission also recommends the establishment of a National Counterterrorism Center (“NCTC”) which focuses all-source intelligence, foreign and domestic, on transnational terrorist organizations. I note briefly in passing that it is important, for fundamental privacy and civil liberties concerns, that, as with the existing Terrorist Threat Integration Center (“TTIC”), intelligence relating to purely domestic organizations, even violent ones, **NOT** be a part of NCTC. The Federal Bureau of Investigation is very capable of dealing with the threat to public safety posed by these organizations.

### **CALEA: Ensuring that Technological Advances not Provide a Safe Haven for Terrorists**

Technology advances, however, may render some provisions of the Patriot Act, especially those that deal with electronic surveillance, moot. Congress contemplated this possibility in 1994 when it enacted the Communication Assistance for Law Enforcement Act (CALEA). CALEA became the law because of concerns that advances in telecommunications technology could limit the effectiveness of lawful electronic surveillance.

It is critically important to understand that CALEA does not give law enforcement any new or augmented authority to conduct court ordered electronic surveillance. Rather, CALEA provides law

enforcement with the technical capability to conduct court ordered electronic surveillance by requiring industry to develop and make operational CALEA intercept capabilities. In other words, the equipment utilized by telecommunications carriers must have the capability of allowing, for example, wiretap devices to be installed on it after, and only after, law enforcement has obtained an order from a court authorizing it to intercept the communications of terrorists or criminals identified in the order.

Unfortunately, CALEA has not achieved its laudable objectives. In a recent and excellent report, the Department of Justice's Inspector General found that nine years after the legislation was enacted, CALEA technical solutions for electronic surveillance remain significantly delayed. The Inspector General's report details the reasons for the delays in CALEA implementation, including delays in establishing industry electronic surveillance standards through the Federal Communications Commission. The report ominously notes that emerging technologies for which electronic surveillance standards are inadequate or not yet developed will further complicate the full implementation of CALEA. The Inspector General made three recommendations to improve CALEA implementations, the most important of which was for the Department of Justice to submit to Congress proposed legislation "necessary to ensure that lawful electronic surveillance is achieved expeditiously in the face of rapid change."

To spur full CALEA implementation, the Department of Justice has filed with the Federal Communications Commission a petition for expedited rulemaking. Among the several issues that the petition asks the Commission to resolve, the most important is Justice's request that the Commission find that broadband access services and broadband telephony services are subject to CALEA.

Justice's proposal has received well-meaning but spirited opposition. The focus of the opposition is that CALEA does not apply to information services such as email and voice over internet protocol or VoIP.

This seeming ambiguity concerning the scope of CALEA needs to be resolved. It is clearly detrimental to the nation's security interests. Consider the following possibility that is not far-fetched, given the Inspector General's finding that CALEA technical solutions and compliance has not yet been fully implemented. You have a provider whose equipment law enforcement needs to utilize quickly because of information it has received regarding communications involving individuals taking part in a terrorist plot. In other words, you have the classic "ticking bomb" scenario. If the provider does not have adequate interception capability, a Title III or FISA order cannot be implemented in a timely manner. Government engineers will have to work with the provider's engineers to find a workable electronic surveillance/interception solution and before any court order can be implemented. This wasted time subjects the public safety of Americans to unnecessary risk.

In a pleading filed before the Federal Communication Commission, the Department of Justice has eloquently noted the catastrophic consequences of this risk:

Today, in the context of coordinated terrorist attacks which may result in the loss of life for hundreds or thousands of Americans, any unnecessary delay is simply inexcusable. The finer nuances...between circuit switched and packet-mode telephony will be lost on the surviving family members of the victims should a terrorist attack occur in the breach between the issuance of an order and its delayed implementation because of either non-coverage or non-compliance with CALEA.

The Commission has urged the nation to take immediate steps to prevent future terrorist attacks against the homeland. This urgency is equally applicable to CALEA. The Inspector General recommended that legislative changes be developed that are necessary to ensure that lawful electronic surveillance is achieved expeditiously in the face of rapid technological change." This

recommendation should be carried out with dispatch. The Federal Bureau of Investigation is currently preparing a legislative recommendation for review by Justice and the White House. The FBI then plans to brief appropriate members of Congress on the need for a legislative remedy for delays in CALEA implementation. The FBI states that all this can be done during 2004. This process must be completed within the projected time frame. And when Congress receives the Administration's proposals it should act on them with the same sense of urgency that it is approaching the proposals of the 9/11 Commission. The public safety of our nation, and even the lives of its citizens, may depend on Congress' expeditious response.