

STATEMENT OF

**J. PATRICK ROWAN
PARTNER, MCGUIREWOODS LLP**

BEFORE THE

**COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY**

HEARING ON: "THE USA PATRIOT ACT: DISPELLING THE MYTHS"

PRESENTED ON

MAY 11, 2011

Chairman Sensenbrenner, Ranking Member Scott, and members of the Subcommittee, thank you for inviting me to testify today. My name is Patrick Rowan, and I am currently a partner in the law firm of McGuireWoods LLP. Prior to joining the firm in 2009, I worked at the Department of Justice (DOJ) for eighteen years. Many of those years were spent as a federal prosecutor, but the last portion of my time at DOJ was spent in positions with national security responsibilities, including at the FBI Office of General Counsel, the Criminal Division and then the National Security Division (NSD).

During this period, I had the opportunity to work with FBI agents and DOJ lawyers who dedicated their days and nights to countering the national security threats that face our country. In this work, the investigative tools drawn from the USA PATRIOT Act (PATRIOT Act) were regularly and responsibly deployed in the service of our national security. Even though the provisions of the PATRIOT Act have been repeatedly and successfully used in national security investigations over the last nine and a half years, the Act remains somewhat controversial. While there is great value in the ongoing national dialogue about the balance between liberty and security, I believe that at least some of the continuing concern about the PATRIOT Act stems from misconceptions that have grown up around the Act.

Accordingly, I appreciate the opportunity to appear before this Committee to address some of these misconceptions. In my remarks I will try to focus most specifically on misconceptions relating to the three provisions of the Foreign Intelligence Surveillance Act (“FISA”) that are scheduled to sunset this month: the “roving” surveillance provision, the “business records” provision and the “lone wolf” definition.

There is nothing about these three provisions, Sections 206 (roving) and 215 (business records) of the PATRIOT Act and Section 6001(a) (lone wolf) of the Intelligence Reform and Terrorism Prevention Act, to suggest that they are particularly susceptible to misuse. On the contrary, each of the provisions is subject to substantial protections against civil rights abuses. Each requires the Government to make a showing to an independent court, the FISA court. Each provision comes with rules governing how the Government handles information regarding United States persons. And each is subject to extensive executive branch oversight, as well as congressional reporting requirements.

The Government’s most recent statements indicate that the lone wolf definition has never been used, let alone abused. The two other tools, which have been used, hardly represent radical incursions on civil liberties. These tools were recognized as available for ordinary criminal investigations long before 9/11. Law enforcement agencies have had similar roving authority for Title III wiretaps since 1986, and the authority has repeatedly been upheld in the courts. *See, e.g., United States v. Gaytan*, 74 F.3d 545, 553 (5th Cir. 1996); *United States v. Bianco*, 998 F. 2d 1112, 1122-1123 (2d Cir. 1993). The business records that the government seeks to obtain through a Section 215 order can be

obtained with a garden variety grand jury subpoena in a conventional criminal investigation.

Criminal Investigations Compared With National Security Investigations

Some apparently believe that the Government uses these national security tools to make an end-run around the judiciary and other forms of oversight that exist on the criminal law enforcement side. I think that notion overstates the protections on the criminal side and understates the protections on the national security side.

For example, as I already noted, a FISA business records order is used to obtain the same records that can be acquired with a grand jury subpoena. As a federal prosecutor, I issued grand jury subpoenas to specific individuals and organizations with virtually no oversight and no meaningful judicial review. The recipient of such a subpoena was required to comply with its demands whenever there was a “reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.” *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

Because those records were acquired in the course of a grand jury investigation, the person to whom those records pertained was ordinarily not aware that the government had obtained them. Those records did not necessarily relate directly to the target of the investigation. For example, in a fraud or bribery investigation, it would certainly not be unusual to seek records relating to the target’s girlfriend to determine if her activities had some relation to the target’s crimes. If the grand jury did not return an indictment or the charged offenses were not connected to the girlfriend’s activities, the girlfriend would likely never learn that her records had been subpoenaed.

To employ the FISA business records provision, the Government must apply to an independent court and demonstrate relevance in order to obtain a court order under the provision. There are heightened protections when investigators seek materials that are considered especially sensitive, such as medical records and records from libraries or bookstores. If the target of the investigation is a U.S. person, the Government must show that the investigation is not based solely on activities protected by the First Amendment. *See* 50 U.S.C. § 1861(a)(1), (a)(2)(B). Moreover, the Government must adhere to minimization procedures that limit the retention and dissemination of the information that is obtained concerning U.S. persons. *See* 50 U.S.C. § 1861(b)(2)(B) and (g). The Government must also report to Congress on the use of this tool.

To the extent that one assumes that criminal investigative tools are used with greater care because investigators understand that they will eventually have to defend their actions in a court, one must keep in mind that national security investigations often result in prosecutions as well. Agents know that even the most sensitive national security investigation may ultimately end up in court, where the investigative techniques will be scrutinized. This is particularly true when the investigation targets a U.S. person. Agents understand that the most obvious and effective tool for neutralizing a U.S. person who

threatens our security is a federal criminal prosecution, and they make decisions about the use of investigative tools with that principle in mind.

While there are thousands and thousands of grand jury subpoenas issued every year, the National Security Division recently disclosed that the business records provision is used about forty times per year on average. There is nothing about these numbers that suggests the business records provision is being abused.

The business records provision is not as fast or convenient as a grand jury subpoena. As a result, agents do not ordinarily elect to seek them except in those circumstances in which the secrecy of the investigation is paramount. The business records provision bars the recipient from disclosing it, although the recipient may challenge the non-disclosure requirement in court (as well as the validity of the order).

The secrecy provisions surrounding these authorities are a critical element of their utility. Given the high stakes in national security investigations, it is essential that the investigations be conducted in secret, so that the targets do not adopt countermeasures to avoid detection.

In this regard, the criminal law analogues to our FISA tools – Title III wiretaps, grand jury subpoenas and criminal search warrants – are simply not an acceptable substitute. The procedural requirements imposed by the criminal law, which for Title III wiretaps include mandatory disclosure to the target at the conclusion of the wiretap, make it impossible to conduct long-running intelligence-gathering investigations and increase the likelihood that an investigation will be compromised in the short term.

The Lone Wolf Definition Remains Necessary

The Government recently indicated that it has never had occasion to use the “lone wolf” definition, contained in Section 1801(b)(1)(C) of Title 50 and added in 2004. This provision, which applies only to non-U.S. persons, allows the Government to conduct surveillance and physical search of individuals engaged in international terrorism without demonstrating that they are affiliated with a particular international terrorist group.

There are some who argue that the non-use of the lone wolf definition demonstrates that this provision is unnecessary and that it should be allowed to expire. I don't subscribe to this logic. The mere fact that I have never had occasion to use my spare tire does not mean that I would prefer not to have one in my car. The availability of radicalizing material on the Internet seems to be producing more and more individuals who form the intention to carry out violence on their own, without the aid and support of a terrorist organization. These are the circumstances for which the lone wolf definition was created. If and when the need for the lone wolf definition arises, it should be available to the FBI and their partners at NSD; valuable time and resources might be wasted in trying to engineer a work-around for the lapsed definition.

The FISA Judges Conduct Meaningful Review

Many of those who are concerned about the PATRIOT Act seem to think that the judges of the FISA Court are rubber-stamps for the government, that these judges approve everything that they are asked to approve and impose no meaningful check on the government. From personal experience, I can tell you that this simply is not true.

The judges who sit on the FISA Court are well aware that they only hear the government's side of the story. This is not an unfamiliar posture for any federal judge, because they are regularly called upon to review *ex parte* requests for search warrants, arrest warrants, and Title III electronic surveillance. They understand that a one-sided recitation of allegations requires extra scrutiny, and the FISA judges bring that understanding with them to the Court.

The judges of the FISA Court conduct a meaningful review of each application that is submitted to them. The judges often require additional information and changes and modifications to the proposed orders. Moreover, the judges regularly require reporting as to whether their orders are being followed. The Government's lawyers and agents understand that the FISA Court expects to hear if its orders have been violated, even if the violation was inadvertent.

The Value of Oversight

Over and above the requirements of the FISA Court, the Executive Branch conducts its own oversight of FISA-related intelligence-gathering activities. Each FISA application is subject to close scrutiny by the FBI and the NSD and must be approved by one of a small number of officials before it is submitted to the FISA Court. The FBI's use of FISA authorities is also subject to oversight by the NSD, the DOJ's Office of Inspector General (OIG) and the Office of the Director of National Intelligence. In addition, Congress receives regular reports and copies of significant FISA Court opinions. Thus, there are a number of entities that seek to ensure that these authorities are used in compliance with the law and in a manner that protects privacy and civil liberties.

These oversight mechanisms have real value, as was demonstrated in connection with the FBI's use of National Security Letters (NSLs). As you know, the PATRIOT Act changed the standard of proof required to use NSLs, permitting their use when the material sought by the NSL is relevant to a national security investigation. This change and others, combined with the changing threat environment, resulted in dramatically expanded use of NSLs by the FBI.

In reauthorizing the PATRIOT Act in 2006, the Congress revised the NSL provisions to permit recipients to challenge the NSLs and their nondisclosure provisions and to require the DOJ's OIG to review the FBI's use of NSLs for potential misuse.

Thereafter, the DOJ's OIG issued a report that was critical of the FBI's use of NSL authorities. A 2007 report exposed a number of problems, including that NSLs were issued out of "control files," rather than from "investigative files," in violation of FBI policy. In his report, the Inspector General explained that "in most – but not all of the cases we examined in this review, the FBI was seeking information that it could have obtained properly through national security letters if it had followed applicable statutes, guidelines, and internal policies. *See* Statement of Glenn A. Fine, Inspector General, U.S. Department of Justice, before the House Judiciary Committee concerning the FBI's Use of National Security Letters and Section 215 Requests for Business Records," (March 20, 2007) at 4. The Inspector General also found that FBI agents had not intentionally sought to misuse NSLs but that the misuses were the product of mistakes, carelessness, confusion, sloppiness, lack of training, lack of guidance, and lack of adequate oversight." *Id.*

In response to this report, the FBI developed an automated process for the issuance of NSLs, to ensure that all applicable legal and administrative requirements are met before the NSL goes out. One of these requirements is review and approval by an FBI attorney. The processing system has also improved the FBI's ability to accurately report NSL use to Congress.

The FBI also tightened its policies regarding the use of NSLs and published comprehensive guidance for agents on their use. Extensive training on the use of NSLs has been conducted at FBI Headquarters and in field offices. The FBI's Inspections Division began conducting NSL audits, and the Bureau established an Office of Integrity and Compliance that aids in assessing compliance with NSL policies and procedures. Finally, lawyers from NSD and the FBI conduct oversight of FBI field offices each year through National Security Reviews ("NSRs"). The NSR teams ordinarily visit 15-20 field offices each year and perform comprehensive reviews of the field office's use of NSLs, among other things.

In a follow-on report before all these improvements were in place, the Inspector General found that the FBI and DOJ had made "significant progress" in implementing recommendations from the 2007 report. Department of Justice Office of Inspector General Report, "A Review of the FBI's Use of National Security Letters: Assessment of NSL Usage in 2006" (March 2008). With the full implementation of the mechanisms outlined above, I have little doubt that compliance has further improved.

I cite this history of NSL flaws and fixes to demonstrate that oversight is meaningful, and problems do get identified and fixed, even when they arise in a secret environment. The Congress, the DOJ and the FBI recognize the value of our national security investigative tools and they take care to police their use of the tools.

Conclusion

In conclusion, I want to thank you for the opportunity to appear before you to discuss the USA PATRIOT Act. The three provisions that are set to expire constitute

important tools for use in a narrow class of national security investigations. I appreciate your desire to identify and strip away any misconceptions that serve to complicate the important task of reviewing their utility. I would be happy to answer any questions that you might have.