Department of Justice

STATEMENT

OF

STATEMENT OF
TODD M. HINNEN
ACTING ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"USA PATRIOT ACT REAUTHORIZATION"

PRESENTED ON
MARCH 9, 2011

Statement of
Todd M. Hinnen
Acting Assistant Attorney General
Department of Justice
Before the
Subcommittee on Crime, Terrorism and Homeland Security
Committee on the Judiciary
United States House of Representatives
At a Hearing Entitled
"USA PATRIOT Act Reauthorization"
Presented on
March 9, 2011

Chairman Sensenbrenner, Ranking Member Scott, and members of the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, thank you for inviting me to testify today concerning the three provisions of the Foreign Intelligence Surveillance Act ("FISA") that were recently reauthorized but are scheduled to sunset again in May. Two of these provisions have been part of FISA since the USA PATRIOT Act was enacted nearly a decade ago, and the third has been in FISA since 2004. They have all been reauthorized several times since enactment. As you know, we continue to believe these are critical tools for national security investigations that facilitate the collection of vital foreign intelligence and counterintelligence information. Consequently, we strongly support their continued reauthorization. The Attorney General and Director of National Intelligence have written to the leadership of both houses of Congress urging that Congress grant a reauthorization of sufficient duration to provide those charged with protecting our nation with reasonable certainty and predictability.

Today I will briefly describe the three expiring provisions (the "roving" surveillance provision, the "lone wolf" definition, and the "business records" provision), explain how they have typically been used in practice, and identify some of the safeguards that ensure that these authorities are used responsibly.

Roving Surveillance

FISA's "roving" electronic surveillance provision allows the Government to continue surveillance where the target of the surveillance switches from a facility (*e.g.*, a telephone) associated with one service provider (*e.g.*, a telephone company) to a different facility associated with a different provider. This provision, now codified at 50 U.S.C. § 1805(c)(2)(B), was enacted in the USA PATRIOT Act to correspond to roving authority that has applied to law-enforcement surveillance since 1986. *See* 18 U.S.C. § 2518(11).

To explain the significance of FISA's roving surveillance provision, I need first to describe how FISA functions in ordinary, non-roving cases, and then highlight the differences in roving cases. In an ordinary FISA surveillance case, the Government must demonstrate to the FISA Court probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that he is using, or about to use, a facility, such as a telephone. *See* 50 U.S.C. §1805(a)(2).

If it finds probable cause and approves the Government's application, the FISA Court then issues two separate orders. One order goes to the Government, and actually authorizes the surveillance. The other, referred to as a "secondary" order, goes to the provider – the telephone company – and directs it to assist the Government in conducting the surveillance. *See* 50 U.S.C. § 1805(c)(1)-(2). The secondary order is necessary because, in most cases, we need the affirmative assistance of the phone company to implement the surveillance. In an ordinary case, if the target switches to a new provider the Government must submit a new application and obtain a new set of FISA orders, because the new provider will – rightly – refuse to honor a secondary order directed at another company. However, where the Government can demonstrate in advance to the FISA Court that the *target's actions may have the effect of thwarting surveillance, such as by changing providers*, FISA's roving surveillance provision allows the FISA Court to issue a generic secondary order that we can serve on the new provider to commence surveillance without first going back to Court. The Government's probable cause showing that the target is an agent of a foreign power remains the same, and the Government must also demonstrate to the FISA Court, normally within 10 days of initiating surveillance of the new facility, probable cause that that specific agent is using, or is about to use, that new facility.

This provision is, as noted above, modeled on similar "roving" authority that has applied to law enforcement wiretaps since 1986 and has repeatedly been upheld in the courts. *See, e.g.*, *United States v. Jackson*, 207 F.3d 910, 914 (7th Cir. 2000), *vacated on other grounds*, 531 U.S. 953 (2000); *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); *United States v. Petti*, 973 F.2d 1441, 1445 (9th Cir. 1992). These courts have expressly rejected the argument that roving surveillance violates the Fourth Amendment's "particularity" requirement.

In sum, there are three key points with respect to roving authority: first, in a roving case, just as in an ordinary case, the Government must establish (and the Court must find) probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and only that particular target's use of a new facility will justify a roving wire tap. *See* 50 U.S.C.
§ 1805(a)(2). Even where we do not know the target's name, we must provide the court sufficient detail to identify him with particularity. Second, we can obtain roving authority only where the FISA Court "finds, based upon specific facts in the application," that the actions of the target "may have the effect of thwarting" our ability to conduct surveillance with the aid of a specified provider or other third party. *See* 50 U.S.C. § 1805(c)(2)(B). Third, whenever we implement roving authority, we must report to the FISA Court, normally within 10 days, with the probable cause that ties the target to the new facility. *See* 50 U.S.C. § 1805(c)(3).

The authority to conduct roving electronic surveillance under FISA has proven operationally useful in a small but steady number of national security investigations each year. Typically, these situations involve highly-trained foreign intelligence officers operating in the United States, or other investigative subjects who have already shown an

apparent propensity to evade electronic surveillance. Between 2001 and 2010, the Government has sought roving surveillance authority in about 20 cases per year, on average.

Lone Wolf

The next expiring provision is the so-called "lone-wolf" definition, contained in section 1801(b)(1)(C) of Title 50. This definition allows us to conduct surveillance and physical search of *non-U.S. persons* engaged in international terrorism without demonstrating that they are affiliated with a particular international terrorist group.

There are two key points to understand about this provision. First, it applies only to non-U.S. persons (not to American citizens or green-card holders), *see* 50 U.S.C. § 1801(b)(1)(C), and only when they engage or prepare to engage in "international terrorism." *See* 50 U.S.C.
§ 1801(c). In practice, the Government must know a great deal about the target, including the target's purpose and plans for terrorist activity (in order to satisfy the definition of "international terrorism"), but need not establish probable cause to believe the target is engaging in those activities for or on behalf of a foreign power..

Second, although we have not used this authority to date, it is designed to fill an important gap in our collection capabilities by allowing us to collect on an individual foreign terrorist who is inspired by – but not a member of – a terrorist group. For example, it might allow surveillance when an individual acts based upon international terrorist recruitment and training on the internet without establishing a connection to any terrorist group. It might also be used when a member of an international terrorist group, perhaps dispatched to the United States to form an operational cell, breaks with the group but nonetheless continues to plot or prepare for acts of international terrorism. If such cases arise, which seems increasingly likely given the trend toward independent extremist actors who "self-radicalize," we might have difficulty obtaining FISA collection authority without the lone-wolf provision.

Business Records

The third expiring provision is the so-called "business records" provision, enacted in section 215 of the USA PATRIOT Act. This part of the statute allows the Government to apply to the FISA Court for an order directing the production of business records or tangible things that are relevant to an authorized national security investigation. *See* 50 U.S.C. § 1861. This authority allows the Government to obtain under FISA in a national security investigation the same types of records that can be obtained by a grand jury subpoena in an ordinary criminal investigation, though unlike a grand jury subpoena, it requires an order from the FISA Court. *See* 50 U.S.C. § 1861(c)(2)(D).

Section 215 has been used to obtain driver's license records, hotel records, car rental records, apartment leasing records, credit card records, and the like. It has never been used against a library to obtain circulation records. Some orders have also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately briefed. On average, we seek and obtain section 215 orders less than 40 times per year. Many of these are cases where FBI

investigators need to obtain information that does not fall within the scope of authorities relating to national security letters and are operating in an environment that precludes the use of less secure criminal authorities.

To obtain a business records order from the Court, the Government generally must show three main things. First, the Government must show that it is seeking the information in certain authorized national security investigations conducted pursuant to guidelines approved by the Attorney General. *See* 50 U.S.C. § 1861(a)(2)(A). Second, where the investigative target 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). Third, the Government must show that the information sought is relevant to the authorized investigation. *See* 50 U.S.C. § 1861(b)(2)(A). In addition, under the language of section 215, 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 business records provision also bars the recipient of a business records order from disclosing it. However, the recipient of the order may challenge its legality, as well as any non-disclosure requirement, in court. To date, no recipient of a FISA business records order has challenged the validity of the order or a non-disclosure requirement.

Some have argued that section 215 runs afoul of the Fourth Amendment because it allows the Government to obtain records upon a showing of "relevance" to an authorized investigation rather than "probable cause." However, for constitutional purposes, a business records order is not a "search" within the meaning of the Fourth Amendment. It does not authorize the Government to enter premises and seize records or other tangible things. Instead, like a grand jury subpoena or administrative subpoena, it requires the recipient to identify the responsive items and provide them to the Government. Therefore, the probable cause requirement is inapplicable in this context. *Cf. Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) (grand jury subpoenas "do not require proof of probable cause"); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186 (1946) (orders for the production of records "present no question of actual search and seizure"). The "relevance" standard for business records orders under FISA parallels the standards that Congress has authorized for administrative subpoenas in health care fraud. *See* 18 U.S.C. § 3486; 21 U.S.C. § 876. In addressing administrative subpoenas, the Supreme Court has explained that "[i]t is not necessary, as in the case of a warrant, that a specific charge or complaint of violation of law be pending or that the order be made pursuant to one. It is enough that the investigation be for a lawfully authorized purpose, within the power of Congress to command." *Oklahoma Press Pub. Co.*, 327 U.S. at 208-09.

****

In closing, we continue to believe that these three authorities are critical to national security investigations and should be reauthorized for a period that will provide our intelligence professionals confidence that these important tools will continue to be available to protect national security. Robust substantive standards and procedural protections are in place to ensure that these tools are used responsibly and in a manner that safeguards Americans' privacy and civil liberties. All three authorities require

approval of the FISA Court before they can be used. If Congress feels that there are ways that those protections can be further enhanced while maintaining the effectiveness of these and other intelligence tools, we remain open to such measures.

Thank you again for inviting me to this hearing and I am happy to answer any questions you may have.