



Department of Justice

STATEMENT

OF

MARY BETH BUCHANAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF PENNSYLVANIA

BEFORE THE

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

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PART I:
(USA PATRIOT ACT §§ 204, 207, 214, 225 & THE "LONE WOLF" PROVISION)

PRESENTED ON

APRIL 26, 2005

MARY BETH BUCHANAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF PENNSYLVANIA
PREPARED REMARKS FOR THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

APRIL 26, 2005

INTRODUCTION

Mr. Chairman, Ranking Member Scott, Members of the Subcommittee, thank you for asking me here today. I am Mary Beth Buchanan, the United States Attorney in the Western District of Pennsylvania and the Director of the Executive Office for United States Attorneys. It is an honor to appear before you today to discuss how the Department has used the important provisions of the USA PATRIOT Act to better combat terrorism and other serious criminal conduct. I will specifically focus today on two of the provisions that are the subject of today's hearing – Section 214 and Section 225 of the USA PATRIOT Act – since those are two provisions that harmonized tools used in terrorism investigations with tools that have been used routinely and effectively in criminal prosecutions long before the passage of the USA PATRIOT Act.

Section 214 of the USA PATRIOT Act allows the government to obtain a pen register order in national security investigations where the information likely is relevant to an international

terrorism or espionage investigation. This provision is similar to the 1986 criminal pen register statute (18 U.S.C. § 3121) that has been frequently used by criminal prosecutors to obtain pen registers and trap and trace devices in a variety of criminal investigations. A pen register is a device that can track dialing, routing, addressing, and signaling information about a communication – for example, which numbers are dialed from a particular telephone. Pen registers are not used to collect the content of communications. Similarly, a trap-and-trace device tracks numbers used to call a particular telephone, without monitoring the substance or content of the telephone conversation. Both devices are routinely used in criminal investigations where, in order to obtain the necessary order authorizing use of the device, the government must show simply that the information sought is relevant to an ongoing investigation.

Pen registers and trap and trace devices have long been used as standard preliminary investigative tools in a variety of criminal investigations and prosecutions. In many instances, these tools are used as one of the first steps in a criminal investigation with the information gathered used to determine if more intrusive forms of surveillance, such as search warrants or wiretaps, are justified. Use of these tools may oftentimes lead investigators and prosecutors to additional suspects or targets in an investigation because of their important ability to allow prosecutors to link defendants or “connect the dots” in a conspiracy or other type of criminal offense.

To obtain a pen register or trap and trace device under 18 U.S.C. § 3121 *et seq.*, a criminal prosecutor must certify that the information sought is relevant to an ongoing criminal investigation, and upon that certification, the court enters an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device. There is no requirement that the

court make a probable cause finding. Under long-settled Supreme Court precedent, the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment. As such, the Constitution does not require that the government obtain court approval before installing a pen register. The absence of a probable cause requirement is justified because the devices merely obtain information that is voluntarily disclosed to the telephone service provider. Therefore, there is no reasonable expectation of privacy in the information.

Currently under FISA, government officials similarly may seek a court order for a pen register or trap-and-trace device to gather foreign intelligence information or information about international terrorism or espionage. Prior to enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought was relevant to an intelligence investigation, but also that the facilities to be monitored had been used or were about to be used to contact a foreign agent or an agent of a foreign power, such as a terrorist or spy. Thus, it was much more difficult to obtain an effective pen register or trap-and-trace order in an international terrorism investigation than in a criminal investigation.

Section 214 of the USA PATRIOT Act brought authorities for terrorism and other foreign intelligence investigations more into line with similar criminal authorities by permitting court approval of FISA pen registers and trap-and-trace orders even though an applicant might be unable to certify at that stage of an investigation that the facilities themselves, such as phones, are used by foreign agents or those engaged in international terrorist or clandestine intelligence activities. Significantly, however, applicants must still certify that the devices are likely to obtain foreign intelligence information not concerning a U.S. person, or information relevant to an international terrorism investigation. Section 214 streamlined the process for obtaining pen

registers under FISA while preserving the existing court-order requirement that is evaluated by the same relevance standard as in the criminal context. Now as before, investigators cannot install a pen register unless they apply for and receive permission from the FISA Court. In addition, Section 214 explicitly safeguards First Amendment rights. It requires that any investigation of a United States person not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution. As a result, the Department of Justice must satisfy the FISA Court that its investigation is not solely based upon First Amendment protected activity, which requires the Department to inform the Court of the justification for the investigation.

If Section 214 were allowed to expire, it would be more difficult to obtain a pen register order in an international terrorism investigation than in a criminal investigation, and investigators would have a harder time developing leads in important terrorism investigations.

Section 225 of the USA PATRIOT Act also harmonized the FISA context and criminal prosecutions--in this case extending an important provision used for years in criminal prosecutions to the FISA context. The United States may obtain electronic surveillance and physical search orders from the FISA Court concerning an entity or individual whom the court finds probable cause to believe is an agent of a foreign power. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers to carry out such court orders. In the criminal and civil contexts, those who disclose information pursuant to a subpoena or court order are generally exempted from liability. For example, those assisting the government in carrying out criminal investigative wiretaps are provided with immunity from civil liability. This immunity is important because it

helps to secure the prompt cooperation of private parties with law enforcement officers to ensure the effective implementation of court orders.

Prior to the passage of the USA PATRIOT Act, however, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out surveillance orders issued by the FISA Court under FISA. Section 225 ended this anomaly by providing immunity to those who assist the government in implementing FISA surveillance orders, thus ensuring that such entities and individuals will comply with orders issued by the FISA Court without delay. This immunity is important because it helps to secure the prompt cooperation of private parties, such as telephone companies, whose assistance is necessary for the effective implementation of court orders. For example, in the investigation of an espionage subject, the FBI was able to convince a company to assist in the installation of technical equipment pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. Section 225 has been praised for protecting those companies and individuals who are simply fulfilling their legal obligations. If section 225 is allowed to expire, it would be more difficult for the Department of Justice to implement FISA surveillance orders in a timely and effective manner. Because Section 225 simply extends to the FISA context the exemption long applied in the civil and criminal contexts, where individuals who disclose information pursuant to a subpoena or court order generally are immune from liability for disclosure, it should be made permanent.

I thank you for inviting me here and giving me the opportunity to explain in concrete terms how the USA PATRIOT Act has changed the way we fight terrorism. I hope you agree that there is no good reason for investigators to have fewer tools to use in terrorism investigations than they have long used in criminal investigations. Fortunately, the USA PATRIOT Act was passed by Congress to correct these flaws in the system. Now that we have fixed this process, we can't go back. We must continue to pursue the terrorists with every legal means available. The law enforcement community needs the important tools of the USA PATRIOT Act to continue to keep our nation safe from attack.

I thank this Committee for its continued leadership and support. I will be happy to respond to any questions you may have.

Testimony of Alberto R. Gonzales, Attorney General of the United States
and Robert S. Mueller, III, Director, Federal Bureau of Investigation
United States Department of Justice
Before the Select Committee on Intelligence
United States Senate
April 27, 2005

Chairman Roberts, Vice Chairman Rockefeller, and Members of the Committee:

We are pleased to be here today to discuss the government's use of authorities granted to it by Congress under the Foreign Intelligence Surveillance Act of 1978 (FISA). In particular, we appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA made by the USA PATRIOT Act and how critical they are to the government's ability to successfully prosecute the war on terrorism and prevent another attack like that of September 11 from ever happening again.

As we stated in our testimony to the Senate Judiciary Committee, we are open to suggestions for strengthening and clarifying the USA PATRIOT Act, and we look forward to meeting with people both inside and outside of Congress who have expressed views about the Act. However, we will not support any proposal that would undermine our ability to combat terrorism effectively.

I. FISA Statistics

First, we would like to talk with you about the use of FISA generally. Since September 11, the volume of applications to the Foreign Intelligence Surveillance Court (FISA court) has dramatically increased.

- In 2000, 1,012 applications for surveillance or search were filed under FISA. As the Department's public annual FISA report sent to Congress on April 1, 2005 states, in 2004 we filed 1,758 applications, a 74% increase in four years.
- Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the FISA court in some substantive way.

II. Key Uses of FISA Authorities in the War on Terrorism

In enacting the USA PATRIOT Act, the Intelligence Authorization Act for Fiscal Year 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with vital tools that it has used regularly and effectively in its war on terrorism. The reforms contained in those measures affect every single application made by the Department for electronic surveillance or physical search of suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information on suspected terrorists. It is because of the key importance of these tools to the war on terror that we ask you to reauthorize the provisions of the USA PATRIOT Act scheduled to expire at the

end of this year. Of particular concern is section 206's authorization of multipoint or "roving" wiretaps, section 207's expansion of FISA's authorization periods for certain cases, section 214's revision of the legal standard for installing and using pen register / trap and trace devices, and section 215's grant of the ability to obtain a Court order requesting the production of business records related to national security investigations.

In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 includes a "lone wolf" provision that expands the definition of "agent of a foreign power" to include a non-United States person, who acts alone or is believed to be acting alone and who engages in international terrorism or in activities in preparation therefor. This provision is also scheduled to sunset at the end of this year, and we ask that it be made permanent as well.

A. Roving Wiretaps

Section 206 of the USA PATRIOT Act extends to FISA the ability to "follow the target" for purposes of surveillance rather than tie the surveillance to a particular facility and provider when the target's actions may have the effect of thwarting that surveillance. In the Attorney General's testimony at the beginning of this month before the Senate Judiciary Committee, he declassified the fact that the FISA court issued 49 orders authorizing the use of roving surveillance authority under section 206 as of March 30, 2005. Use of roving surveillance has been available to law enforcement for many years and has been upheld as constitutional by several federal courts, including the Second, Fifth, and Ninth Circuits. Some object that this provision gives the FBI discretion to conduct surveillance of persons who are not approved targets of court-authorized surveillance. This is wrong. Section 206 did not change the requirement that before approving electronic surveillance, the FISA court must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Without section 206, investigators will once again have to struggle to catch up to sophisticated terrorists trained to constantly change phones in order to avoid surveillance.

Critics of section 206 also contend that it allows intelligence investigators to conduct "John Doe" roving surveillance that permits the FBI to wiretap every single phone line, mobile communications device, or Internet connection the suspect may use without having to identify the suspect by name. As a result, they fear that the FBI may violate the communications privacy of innocent Americans. Let me respond to this criticism in the following way. First, even when the government is unsure of the name of a target of such a wiretap, FISA requires the government to provide "the identity, if known, or a description of the target of the electronic surveillance" to the FISA Court prior to obtaining the surveillance order. 50 U.S.C. §§ 1804(a)(3) and 1805(c)(1)(A). As a result, each roving wiretap order is tied to a particular target whom the FISA Court must find probable cause to believe is a foreign power or an agent of a foreign power. In addition, the FISA Court must find "that the actions of *the target* of the application may have the effect of thwarting" the surveillance, thereby requiring an analysis of the activities of a foreign power or an agent of a foreign power that can be identified or described. 50 U.S.C.