U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 14, 2009

The Honorable Dianne Feinstein
Chairwoman
The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Senators Feinstein and Bond:

Thank you for your letter requesting our recommendations on the three provisions of the Foreign Intelligence Surveillance Act ("FISA") currently scheduled to expire on December 31, 2009. We believe that the best legislation will emerge from a careful examination of these matters. In this letter, we provide our recommendations for each provision, along with a summary of the supporting facts and rationale. We have discussed these issues with the Office of the Director of National Intelligence, which concurs with the views expressed in this letter.

We also are aware that Members of Congress may propose modifications to provide additional protection for the privacy of law abiding Americans. As President Obama said in his speech at the National Archives on May 21, 2009, "We are indeed at war with al Qaeda and its affiliates. We do need to update our institutions to deal with this threat. But we must do so with an abiding confidence in the rule of law and due process; in checks and balances and accountability." Therefore, the Administration is willing to consider such ideas, provided that they do not undermine the effectiveness of these important authorities.

1. Roving Wiretaps, USA PATRIOT Act Section 206 (codified at 50 U.S.C. § 1805(c)(2))

We recommend reauthorizing section 206 of the USA PATRIOT Act, which provides for roving surveillance of targets who take measures to thwart FISA surveillance. It has proven an important intelligence-gathering tool in a small but significant subset of FISA electronic surveillance orders.

This provision states that where the Government sets forth in its application for a surveillance order "specific facts" indicating that the actions of the target of the order "may have the effect of thwarting" the identification, at the time of the application, of third parties necessary to accomplish the ordered surveillance, the order shall direct such third parties, when identified to furnish the Government with all assistance necessary to accomplish surveillance of the target identified in the order. In other words, the "roving" authority is only available when the

Government is able to provide specific information that the target may engage in counter-surveillance activity (such as rapidly switching cell phone numbers. The language of the statute does not allow the Government to make a general, "boilerplate" allegation that the target may engage in such activities; rather, the Government must provide specific facts to support its allegation.

There are at least two scenarios in which the Government's ability to obtain a roving wiretap may be critical to effective surveillance of a target. The first is where the surveillance targets a traditional foreign intelligence officer. In these cases, the Government often has years of experience maintaining surveillance of officers of a particular foreign intelligence service who are posted to locations within the United States. The FBI will have extensive information documenting the tactics and tradecraft practiced by officers of the particular intelligence service, and may even have information about the training provided to those officers in their home country. Under these circumstances, the Government can represent that an individual who has been identified as an officer of that intelligence service is likely to engage in counter-surveillance activity.

The second scenario in which the ability to obtain a roving wiretap may be critical to effective surveillance is the case of an individual who actually has engaged in counter-surveillance activities or in preparations for such activities. In some cases, individuals already subject to FISA surveillance are found to be making preparations for counter-surveillance activities or instructing associates on how to communicate with them through more secure means. In other cases, non-FISA investigative techniques have revealed counter-surveillance preparations (such as buying "throwaway" cell phones or multiple calling cards). The Government then offers these specific facts to the FISA court as justification for a grant of roving authority.

Since the roving authority was added to FISA in 2001, the Government has sought to use it in a relatively small number of cases (on average, twenty-two applications a year). We would be pleased to brief Members or staff regarding actual numbers, along with specific case examples, in a classified setting. The FBI uses the granted authority only when the target actually begins to engage in counter-surveillance activity that thwarts the already authorized surveillance, and does so in a way that renders the use of roving authority feasible.

Roving authority is subject to the same court-approved minimization rules that govern other electronic surveillance under FISA and that protect against the unjustified acquisition or retention of non-pertinent information. The statute generally requires the Government to notify the FISA court within 10 days of the date upon which surveillance begins to be directed at any new facility. Over the past seven years, this process has functioned well and has provided effective oversight for this investigative technique.

We believe that the basic justification offered to Congress in 2001 for the roving authority remains valid today. Specifically, the ease with which individuals can rapidly shift between communications providers, and the proliferation of both those providers and the services they offer, almost certainly will increase as technology continues to develop. International terrorists, foreign intelligence officers, and espionage suspects — like ordinary criminals — have learned to use these numerous and diverse communications options to their advantage. Any effective surveillance mechanism must incorporate the ability to rapidly address an unanticipated change in the target's communications behavior. The roving electronic surveillance provision has functioned as intended and has addressed an investigative requirement that will continue to be critical to national security operations. Accordingly, we recommend reauthorizing this feature of FISA.

2. "Business Records," USA PATRIOT Act Section 215 (codified at 50 U.S.C. § 1861-62)

We also recommend reauthorizing section 215 of the USA PATRIOT Act, which allows the FISA court to compel the production of "business records." The business records provision addresses a gap in intelligence collection authorities and has proven valuable in a number of contexts.

The USA PATRIOT Act made the FISA authority relating to business records roughly analogous to that available to FBI agents investigating criminal matters through the use of grand jury subpoenas. The original FISA language, added in 1998, limited the business records authority to four specific types of records, and required the Government to demonstrate "specific and articulable facts" supporting a reason to believe that the target was an agent of a foreign power. In the USA PATRIOT Act, the authority was changed to encompass the production of "any tangible things" and the legal standard was changed to one of simple relevance to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

The Government first used the USA PATRIOT Act business records authority in 2004 after extensive internal discussions over its proper implementation. The Department's inspector general evaluated the Department's implementation of this new authority at length, in reports that are now publicly available. Other parts of the USA PATRIOT Act, specifically those eliminating the "wall" separating intelligence operations and criminal investigations, also had an effect on the operational environment. The greater access that intelligence investigators now have to criminal tools (such as grand jury subpoenas) reduces but does not eliminate the need for intelligence tools such as the business records authority. The operational security requirements of most intelligence investigations still require the secrecy afforded by the FISA authority.

For the period 2004-2007, the FISA court has issued about 220 orders to produce business records. Of these, 173 orders were issued in 2004-06 in combination with FISA pen

register orders to address an anomaly in the statutory language that prevented the acquisition of subscriber identification information ordinarily associated with pen register information. Congress corrected this deficiency in the pen register provision in 2006 with language in the USA PATRIOT Improvement and Reauthorization Act. Thus, this use of the business records authority became unnecessary.

The remaining business records orders issued between 2004 and 2007 were used to obtain transactional information that did not fall within the scope of any other national security investigative authority (such as a national security letter). Some of these orders were used to support important and highly sensitive intelligence collection operations, of which both Members of the Intelligence Committee and their staffs are aware. The Department can provide additional information to Members or their staff in a classified setting.

It is noteworthy that no recipient of a FISA business records order has ever challenged the validity of the order, despite the availability, since 2006, of a clear statutory mechanism to do so. At the time of the USA PATRIOT Act, there was concern that the FBI would exploit the broad scope of the business records authority to collect sensitive personal information on constitutionally protected activities, such as the use of public libraries. This simply has not occurred, even in the environment of heightened terrorist threat activity. The oversight provided by Congress since 2001 and the specific oversight provisions added to the statute in 2006 have helped to ensure that the authority is being used as intended.

Based upon this operational experience, we believe that the FISA business records authority should be reauthorized. There will continue to be instances in which FBI investigators need to obtain transactional 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. Many of these instances will be mundane (as they have been in the past), such as the need to obtain driver's license information that is protected by State law. Others will be more complex, such as the need to track the activities of intelligence officers through their use of certain business services. In all these cases, the availability of a generic, court-supervised FISA business records authority is the best option for advancing national security investigations in a manner consistent with civil liberties. The absence of such an authority could force the FBI to sacrifice key intelligence opportunities.

3. "Lone Wolf," Intelligence Reform and Terrorism Prevention Act of 2004 Section 6001 (codified at 50 U.S.C. § 1801(b)(1)(C))

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 defines a "lone wolf" agent of a foreign power and allows a non-United States person who "engages in international terrorism activities" to be considered an agent of a foreign power under FISA even though the specific foreign power (*i.e.*, the international terrorist group) remains unidentified. We also recommend reauthorizing this provision.

Enacted in 2004, this provision arose from discussions inspired by the Zacarias Moussaoui case. The basic idea behind the authority was to cover situations in which information linking the target of an investigation to an international group was absent or insufficient, although the target's engagement in "international terrorism" was sufficiently established. The definition is quite narrow: it applies only to non-United States persons; the activities of the person must meet the FISA definition of "international terrorism;" and the information likely to be obtained must be foreign intelligence information. What this means, in practice, is that 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 still be unable to connect the individual to any group that meets the FISA definition of a foreign power.

To date, the Government has not encountered a case in which this definition was both necessary and available, *i.e.*, the target was a non-United States person. Thus, the definition has never been used in a FISA application. However, we do not believe that this means the authority is now unnecessary. Subsection 101(b) of FISA provides ten separate definitions for the term "agent of a foreign power" (five applicable only to non-United States persons, and five applicable to all persons). Some of these definitions cover the most common fact patterns; others describe narrow categories that may be encountered rarely. However, this latter group includes legitimate targets that could not be accommodated under the more generic definitions and would escape surveillance but for the more specific definitions.

We believe that the "lone wolf" provision falls squarely within this class. While we cannot predict the frequency with which it may be used, we can foresee situations in which it would be the only avenue to effective surveillance. For example, we could have a case in which a known international terrorist affirmatively severed his connection with his group, perhaps following some internal dispute. The target still would be an international terrorist, and an appropriate target for intelligence surveillance. However, the Government could no longer represent to the FISA court that he was currently a member of an international terrorist group or acting on its behalf. Lacking the "lone wolf" definition, the Government could have to postpone FISA surveillance until the target could be linked to another group. Another scenario is the prospect of a terrorist who "self-radicalizes" by means of information and training provided by a variety of international terrorist groups via the Internet. Although this target would have adopted the aims and means of international terrorism, the target would not actually have contacted a terrorist group. Without the lone wolf definition, the Government might be unable to establish FISA surveillance.

These scenarios are not remote hypotheticals; they are based on trends we observe in current intelligence reporting. We cannot determine how common these fact patterns will be in the future or whether any of the targets will so completely lack connections to groups that they cannot be accommodated under other definitions. However, the continued availability of the

lone wolf definition eliminates any gap. The statutory language of the existing provision ensures its narrow application, so the availability of this potentially useful tool carries little risk of overuse. We believe that it is essential to have the tool available for the rare situation in which it is necessary rather than to delay surveillance of a terrorist in the hopes that the necessary links are established.

Thank you for the opportunity to present our views. We would be happy to meet with your staff to discuss them. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General