USA PATRIOT Act Expiring Provisions
Summary

The USA PATRIOT Improvement and Reauthorization Act of 2005 made permanent all but two provisions – Section 206 (roving wiretaps) and Section 215 (Foreign Intelligence Surveillance Act (FISA) Business Records Orders). These provisions and a separate provision of the Intelligence Reform and Terrorism Prevention Act of 2004, known as the "lone wolf" provision, will sunset on May 27, 2011. On Thursday, May 12, 2011, the House Judiciary Committee reported H.R. 1800, the FISA Sunsets Reauthorization Act of 2011, favorably to the House by a vote of 22-13. H.R. 1800 permanently reauthorizes the "lone wolf" definition and extends the sunsets for Section 206 roving authority and Section 215 business records to December 31, 2017.

Section 206 authorizes FISA court orders for multipoint or "roving" wiretaps for foreign intelligence investigations. A "roving" wiretap applies to an individual and allows the government to a use a single wiretap order to cover any communications device that the suspect uses or may use. This type of wiretap differs from a traditional criminal wiretap that only applies to a particular phone or computer used by a target. Without roving wiretap authority, investigators would be forced to seek a new court order each time they need to change the location, phone, or computer that needs to be monitored.

Section 215 allows the Federal government to seek approval from the FISA court of orders granting the government access to any tangible items (including books, records, papers, and other documents) in foreign intelligence, international terrorism, and clandestine intelligence cases. The USA PATRIOT Improvement and Reauthorization Act of 2005 contains several protections against abuses of Section 215 authority, including additional Congressional oversight, procedural protections, application requirements, and a judicial review process.

The "lone wolf" provision allows the government to subject an individual terrorist to the same type of surveillance used to monitor foreign intelligence agents or members of an international terrorist organization. Under this provision, terrorists who work on their own cannot escape surveillance despite not being agents of a foreign power or avowed members of an international terrorist group.

Prepared by Congressman Lamar Smith (R-Texas)
Chairman of the House Judiciary Committee

UNITED STATES HOUSE OF REPRESENTATIVES

JUDICIARY COMMITTEE

Chairman Lamar Smith (TX-21)

Business Records Authority Protects Civil Liberties

The Foreign Intelligence Surveillance Act (FISA) authorizes the government to obtain certain business records in foreign intelligence investigations. The business records provision has more strict requirements than grand jury subpoenas used in criminal investigations. Unlike grand jury subpoenas, business records cannot be obtained without approval by a FISA judge.

The records must be for (1) a foreign intelligence investigation not concerning a U.S. person, or (2) international terrorism or clandestine intelligence activities. **BUT** an investigation of a U.S. person cannot be based solely on activities protected by the 1st Amendment, such as exercise of religion or political protest. The government must demonstrate to the FISA judge that there the records sought are relevant to the investigation.

Requests for library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person cannot be obtained unless the application to the FISA judge is first approved by the FBI Director, Deputy Director, or head of the FBI's National Security Branch.

The government must employ minimization requirements – this means ensuring that it does not collect non-foreign intelligence information. And recipients of 215 orders can challenge the order before the FISA court.

Business records authority only allows the government to request documents held by a 3rd party such as a bank, hotel, or car rental agency. Business records cannot be used to acquire the target's personal documents. Business records authority does not authorize the warrantless search of a target's home or other personal property.

Prepared by Congressman Lamar Smith (R-Texas)
Chairman of the House Judiciary Committee

UNITED STATES HOUSE OF REPRESENTATIVES

JUDICIARY COMMITTEE

Chairman Lamar Smith (TX-21)

Roving Authority is Crucial to Fight Modern-Day Terrorism

Roving wiretaps are nothing new. Domestic law enforcement agencies have had roving authority for criminal investigations since 1986. These wiretaps simply allow investigators to surveil a target, regardless of what phone he/she uses.

Disposable cell phones and free email services allow terrorists and spies to thwart detection by simply changing phones or email accounts. Without roving authority, the government is required to return to a FISA judge for a new court order every time a suspected terrorist or spy switches to a new phone or email address, making it easy for them to evade detection.

A FISA Court judge is the only one who can authorize a roving wiretap. The FISA judge supervises FISA wiretaps as they progress to make sure the authority is being used correctly. The government must notify the FISA judge when they begin tracking a new phone or email account.

To obtain a FISA wiretap, the government must (1) establish probable cause that the target of the surveillance is a foreign power or agent of a foreign power **BUT** no U.S. person can be considered a foreign power or agent of a foreign power solely upon the basis of activities protected by the 1st Amendment; (2) probable cause that the device that is tapped is used or about to be used by a foreign power or agent of a foreign power; (3) demonstrate that the information sought is foreign intelligence information; (4) that a significant purpose of the surveillance is to obtain foreign intelligence information; and (5) that such information cannot reasonably be obtained by normal investigative techniques.

To obtain a roving wiretap, the government must meet all of the requirements above plus make an additional showing that the actions of the target may have the effect of thwarting the identification. The government must notify the FISA Court within 10 days after beginning surveillance on a new phone or computer.

UNITED STATES HOUSE OF REPRESENTATIVES

JUDICIARY COMMITTEE

Chairman Lamar Smith (TX-21)

The Threat from Lone Wolf Terrorists is Real

Al Qaeda has changed its tactics, looking to inspire terrorists who are not "members" of Al Qaeda. Terrorists not affiliated with a known terrorist organization are "lone wolves." They share the jihadist goals of al Qaeda but are not following an operational plan handed down by a terrorist group.

Al Qaeda's own magazine, *Inspire*, leaves no doubt about the lone wolf threat. *Inspire* promotes what it calls "open source jihad" – a shift away from coordinated large-scale attacks to individual attacks. The Summer 2010 issue, for example, instructs on how to make a pipe bomb using everyday materials while the Fall 2010 issue promotes using a car to "mow down" a crowd of people.

Prior to 9/11, there was no law allowing for the government to gather intelligence on these lone wolves. An increasing number of attempted terrorist attacks on the U.S. are being carried out by self-radicalized jihadists who adopt an agenda as equally hateful and destructive as a terrorist group.

The law should not create a gaping loop hole for these terrorists simply because they do not belong to an identified group. The lone wolf definition simply brings our national security laws into the 21st century to allow our intelligence officials to answer the modern day terrorist threat.

Lone wolf authority CANNOT be used against a U.S. Citizen or legal permanent resident. It simply amends the definition of "agent of a foreign power" to include individuals engaging in or preparing activities in international terrorism. The definition does not expand or reduce the FISA tools available to the government nor change the procedures necessary to use those tools, including court approval.

Prepared by Congressman Lamar Smith (R-Texas)
Chairman of the House Judiciary Committee

USA PATRIOT ACT Oversight Requirements

The USA PATRIOT Act mandates extensive reporting requirements to Congress.

The government must submit to Congress semiannual reports on all FISA electronic surveillance, including the use of roving authority. The government must also submit to Congress an annual report on all business records orders, including the number of orders granted, modified, or denied for the production of library records, book sales and firearms sales records, tax returns, educational records, and medical records containing information to identify a person.

In addition to the reporting requirements above, on a semiannual basis, the government must submit to Congress a report setting forth for the previous 6 month period the aggregate number of persons targeted for electronic surveillance, physical searches, pen registers, and business records.

The government must also report the number of individuals covered by the lone wolf definition, the number of times the AG has authorized information obtained under FISA be used in criminal proceedings, and copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review.

In April of each year, the government must submit to the Administrative Office of the United States Court and to Congress a report setting forth the total number of applications made for FISA orders and extensions of orders, and the total number of orders and extensions granted, modified, or denied.

Prepared by Congressman Lamar Smith (R-Texas)
Chairman of the House Judiciary Committee