Legal Memorandum
Published by The Heritage Foundation
No. 67
May 24, 2011

Don't Be Misled on Reauthorization of Anti-Terrorism Tools

Andrew M. Grossman

Abstract: *The three anti-terrorism tools scheduled to sunset on May 27, 2011—the authority to conduct "roving" wiretaps of terrorist suspects, to obtain "business records" relating to terrorism investigations, and to conduct surveillance of "lone wolf" terrorist suspects—clearly pass constitutional muster. Each follows the approach, laid out by the courts and by Congress in the Foreign Intelligence Surveillance Act, of allowing the executive to act aggressively while still subjecting executive action to oversight where the domestic activities of foreign powers threaten the nation's safety. To provide certainty in terrorism investigations, Congress should make these tools permanent while continuing to conduct appropriate oversight to ensure that they are used properly.*

Three important tools in the war on terrorism are scheduled to sunset on May 27, 2011. These provisions—the authority to conduct "roving" wiretaps of terrorist suspects, to obtain "business records" relating to terrorism investigations, and to conduct surveillance of "lone wolf" terrorist suspects—were reauthorized last in February, but for only a short duration due in part to some conservative lawmakers' uncertainty over their constitutionality.

A careful examination of their statutory bases, built-in safeguards, historical antecedents, and actual use demonstrates that these powers fall well within the limits on government search and seizure specified in the Constitution and by the courts. Moreover, these are narrowly targeted tools aimed at specific threats

Talking Points

- Concerns that three expiring anti-terrorist tools run afoul of Fourth Amendment requirements are overblown. These tools appropriately balance Fourth Amendment requirements with the President's obligation to protect the nation from foreign threats, and so are constitutional.
- "Roving" wiretaps have been used for years in criminal investigations and have been upheld by the courts. They are an essential tool to keep tabs on individuals who are specifically trained to evade ordinary surveillance techniques.
- "Business records" orders mirror the authority available with grand jury subpoenas, except with greater checks on misuse. They are especially valuable where disclosure would jeopardize a long-running investigation.
- The "lone wolf" definition corrects a small lapse in foreign surveillance authority by allowing the monitoring of individuals with hazy connections to international terrorist groups. In the Internet age, this authority provides an important backstop at the front end of anti-terrorist investigations.

This paper, in its entirety, can be found at:
http://report.heritage.org/lm0067

Produced by the Center for Legal & Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

The Heritage Foundation
LEADERSHIP FOR AMERICA

and threat categories that cannot be ignored in the post-9/11 era.

It would be irresponsible for Congress to allow these tools to expire or to reauthorize them for only a few months, as it did in February. While a four-year reauthorization would provide reasonable certainty to those conducting anti-terrorist intelligence operations, the best course would be to make these provisions permanent while continuing to conduct appropriate oversight to ensure that they are used properly.

Foreign Intelligence and the Fourth Amendment

There is a potential tension between the Fourth Amendment, as it has been applied by the courts, and the President's obligation to protect the nation from national security threats, particularly those arising from the activities of foreign powers, such as terrorist organizations and state sponsors of terrorism. The Fourth Amendment protects against "unreasonable searches and seizures" and sets out requirements for search warrants: "probable cause" and describing with particularity the subject of the warrant or order.

The courts and Congress have harmonized the policies underlying the Fourth Amendment and the President's commander-in-chief power in light of the Framers' intentions and historical practice.

While the Fourth Amendment unambiguously governs criminal investigations, there is great constitutional uncertainty about whether, and to what extent, it applies in the context of the President's role as commander in chief. For example, while U.S. soldiers deployed abroad need not obtain a warrant to seize enemy combatants' records and weapons, the requirements are less certain when an enemy combatant operates within the United States. The courts have never held that mere presence in U.S. territory guarantees Fourth Amendment rights to a foreign intelligence agent or saboteur, but investigations of such individuals do raise risks that Americans' rights may be infringed if foreign intelligence authorities are applied indiscriminately within the United States.

The three anti-terrorist tools up for reauthorization even provide for greater protections than the Constitution requires.

The courts and Congress have resolved this potential tension, however, by harmonizing the policies underlying the Fourth Amendment and the President's commander-in-chief power in light of the Framers' intentions and historical practice. The leading Supreme Court case in this respect is United States v. United States District Court, better known as "Keith," for the federal judge whom the government sought to order to admit evidence obtained by warrantless surveillance of domestic organizations.[1] While holding that the normal Fourth Amendment requirements—probable cause, reasonable particularity, and approval by a neutral and disinterested magistrate—apply to surveillance of domestic national security threats, it recognized that a different rule may apply "with respect to activities of foreign powers or their agents."[2]

Congress expressly adopted this distinction—based on long historical practice predating *Keith*—in the Foreign Intelligence Surveillance Act of 1978, which established a framework outside of the standard warrant requirement for the federal government to obtain approval for and conduct electronic surveillance and, later, physical searches. This framework requires the government to obtain approval by neutral judges (who sit on the Foreign Intelligence Surveillance Court) and to lay out facts justifying the belief that the target is "a foreign power or an agent of a foreign power," as well as "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance."[3]

1. 407 U.S. 297, 299–301 (1972).
2. *Id.* at 321–22.
3. *See* 50 U.S.C. § 1804(a).

Further, with one limited potential exception described below, FISA does not apply at all to a "United States person," which includes U.S. citizens and permanent residents, absent evidence demonstrating that he or she is an agent of a foreign power.[4] In this way, Congress and the courts, which have repeatedly affirmed and upheld the FISA framework, have allowed the executive to act aggressively while still subjecting executive action to oversight where the domestic activities of foreign powers threaten the nation's safety.

The three anti-terrorist tools up for reauthorization follow that model and even provide for greater protections than the Constitution requires. Two are standard tools of the trade in criminal investigations—"roving" wiretaps and "business records" orders—and the third corrects a small loophole in the surveillance authority provided by FISA.

"Roving" Wiretaps

"Roving" wiretaps are nothing remarkable or unprecedented. Since 1986, courts have issued roving "Title III" warrants in criminal investigations, allowing this type of surveillance to collect evidence on players in organized crime and other targets of criminal investigations who have learned that a regular wiretap can be evaded by use of modern technology, switching between prepaid cell phones and various Internet channels for communications.[5] These warrants have been upheld repeatedly by the courts as lawful.[6]

FISA, however, predated the enactment of roving wiretap authority in Title III. This led to the startling incongruity that, while roving wiretaps could be used in criminal investigations, they were unavailable to conduct foreign-intelligence surveillance of individuals who were trained specifically to evade ordinary surveillance techniques.[7] The result was that, as foreign targets skipped between communications devices and services, the agents tracking them were forced to apply for updated surveillance orders, causing breaks in coverage.

Those who imagine that roving wiretaps authorize unbounded surveillance dragnets without any supervision at all are simply misinformed.

The Patriot Act amended FISA to correct this incongruity by authorizing roving wiretaps.[8] The major difference between this authority and that authorized by Title III is that the application, which is submitted to the FISA Court made up of federal judges, need not specify by name the target but can, instead, use other details to identify the particular person subject to surveillance—for example, an Internet handle used on particular Web forums.

Even after the court has approved the application, its oversight continues. The government must inform the court of each device or facility that it taps, specify the "facts justifying a belief that the target is using, or is about to use, that new facility or place," and describe any additional procedures that will be required to "minimize" the information collected—that is, to exclude or discard information that is irrelevant to the investigation.[9] Those who imagine that roving wiretaps authorize unbounded surveillance dragnets without any supervision at all are simply misinformed.

The authorization of roving wiretaps does not alter the FISA framework in any constitutionally meaningful manner. The government must still identify a particular individual for surveillance, the FISA Court must still approve each order, the gov-

4. 50 U.S.C. §§ 1801(i); 1804(a)(3); 1805(a)(2).
5. *See* 18 U.S.C. 2518(11). *See generally* Peter Thomson, White Paper on The USA PATRIOT Act's "Roving" Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act, The Federalist Society, April 2004, at http://www.fed-soc.org/doclib/20070326_rovingsur.pdf.
6. *See, e.g., United States v. Petti*, 973 F.2d 1441 (9th Cir.1992); *United States v. Bianco*, 998 F.2d 1112 (2nd Cir. 1993); *United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States v. Jackson*, 207 F.3d 910 (7th Cir. 2000).
7. *See, e.g., Robert S. Mueller*, FBI Director, Statement for the Record, Joint Intelligence Committee Inquiry (September 25, 2002) (describing evasive techniques of 9/11 hijackers).
8. 50 U.S.C. § 1805(c)(2)(B).
9. 50 U.S.C. §§ 1805(c)(3), 1801(h).

ernment remains obligated to minimize information that does not relate to its investigation, and this entire procedure remains inapplicable to U.S. persons who are not agents of foreign powers. If anything, this authority exceeds constitutional requirements, particularly with respect to the continuing oversight role played by the FISA Court. Moreover, the FISA Court's role helps to ensure that this authority is not misused.

Section 215 "Business Records" Orders

Business records orders are also nothing new or objectionable. In general, the same materials can be obtained with garden-variety grand jury subpoenas issued by the clerk of court rather than by a judge.[10] Indeed, the government routinely relies on grand jury subpoenas to collect information in terrorism cases for the reason that they are faster and more convenient than obtaining business records orders, which requires demonstrating to the FISA Court "reasonable grounds" that the records sought are relevant to an investigation "to protect against international terrorism or clandestine intelligence activities."[11]

Business records orders are also subject to additional restrictions. They are simply unavailable in intelligence investigations targeting a U.S. person where the basis for investigation is "activities protected by the first amendment."[12] Any information collected that concerns U.S. persons is subject to a "minimization" requirement that the government limit its retention and dissemination.[13] And requests for orders seeking sensitive information, like medical records and library records, must be made by high-ranking intelligence officials, ensuring that such requests are made only when absolutely necessary.[14]

Due to these restrictions and the ready availability of alternatives, the government has used this power judiciously. It carries out only about 40 such orders per year, on average.[15] In 2010, the government made 96 applications for Section 215 orders—an uptick after requesting only 21 in 2009—and 43 were modified by the FISA Court before being granted, demonstrating the court's active oversight role.[16]

The reason that terrorism investigators use business records orders at all, despite the procedural hoops, is that they prohibit disclosure of the order by its recipient.[17] The recipient can, however, challenge the non-disclosure requirement, as well as the order itself, in court.[18] The benefit of secrecy in the context of years-long investigations to uncover and disrupt terrorist plots is plain.

The routine use of subpoenas clearly passes Fourth Amendment muster under what is known as the "third-party doctrine."

Such secrecy is hardly unusual in any case. Individuals subject to grand jury subpoenas may never become aware that records pertaining to them were

10. *See, e.g., United States v. R. Enterprises, Inc.*, 498 U.S. 292, 297–99 (1991) ("the Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists."); *id.* at 301 (grand jury subpoena will be quashed only when "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation").
11. *See* 50 U.S.C. § 1861(b)(2)(A).
12. 50 U.S.C. § 1861(a)(1).
13. 50 U.S.C. § 1861(g).
14. 50 U.S.C. § 1861(a)(3).
15. Testimony of J. Patrick Rowan Before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, May 11, 2011, at http://judiciary.house.gov/hearings/pdf/Rowan05112011.pdf.
16. Letter from Ronald Weich, Assistant Attorney General, to Joseph Biden, President, United States Senate (April 30, 2010), at http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf.
17. 50 U.S.C. § 1861(d).
18. 50 U.S.C. § 1861(f)(2)(A)(i).

pulled. As Patrick Rowan, a former federal prosecutor, explained in testimony before a House committee on May 11, it would not be unusual to seek bank records relating to the girlfriend of a target of a federal bribery investigation. If there were ultimately no indictment, or if the charges brought were not connected to her, she would never know that her records had been subpoenaed.[19]

This routine use of subpoenas, of course, clearly passes Fourth Amendment muster under what is known as the "third-party doctrine." As the Supreme Court has explained the doctrine:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[20]

Thus, an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[21]

In constitutional terms, then, Section 215 business records orders are equivalent to grand jury subpoenas, if not even more secure due to the higher standard that the government must satisfy in obtaining them, the specific factual showing it must make, the express limitations contained in the provision itself, and the minimization requirement.

Hunting "Lone Wolves"

The final expiring tool is the "lone wolf" definition, which recognizes that, in the Internet age, the government may be unable to demonstrate at the outset of a terrorism investigation that its target is directly affiliated with a foreign power, such as al-Qaeda. Terrorist groups increasingly use the "franchise" model, in which autonomous groups and individuals located in different areas operate independently with minimal coordination and, in some cases, no hard knowledge of their foreign counterparts. These individuals may be recruited to the cause by online propaganda, inspired to carry out terrorist attacks based on what they read on message boards and news sites, and learn the techniques of terrorism by Googling for technical materials. Unlike in the past, an individual can be part of an international terrorist movement with only the vaguest connection to any specific terrorist group.

That is the basis for the lone-wolf definition. It simply allows the government to apply FISA surveillance to a non-U.S. person who "engages in international terrorism or activities in preparation" for such terrorism, but without proving a direct link to a specific foreign power—which may be impossible in the early stages of an investigation.[22] As with all FISA orders, any lone-wolf investigation is subject to approval by the FISA Court, requires numerous showings and certifications by government officials, and must be subject to minimization procedures to exclude or discard irrelevant information, particularly regarding U.S. persons.

If the "international terrorism" requirement is taken seriously, use of the lone-wolf power runs afoul of no constitutional limitation.

What separates this provision from other portions of FISA is that it does not echo the language used by the Supreme Court in *Keith* concerning "foreign powers or their agents." Critics say this exception to FISA's "foreign power" requirement intrudes on the Fourth Amendment's exclusive domain as identified in *Keith*, but they overlook or downplay the tie that the lone-wolf definition requires to "*international* terrorism,"[23] which is specifically limited in the statute to activities that "occur totally outside the United States, or transcend national boundaries."[24]

19. *See* Rowan, *supra* note 15.
20. *United States v. Miller*, 425 U.S. 435, 443 (1976).
21. *Id*. *See generally* Orin Kerr, The Case for the Third-Party Doctrine, 107 MICH. L. REV. 561 (2009).
22. 50 U.S.C. § 1801(b)(1)(C).
23. 50 U.S.C. § 1801(b)(1)(C).
24. 50 U.S.C. § 1801(c).

While, in hypothetical circumstances, this could be read to slightly broaden the exception to the warrant requirement identified in *Keith*—for example, a lone wolf planning international terrorism is entirely independent of any terrorist organization or other foreign power[25]—as a practical matter, it simply deemphasizes the requirement that the government demonstrate agency at the outset of an investigation. In this sense, it is more a limited clarification of the scope of foreign intelligence surveillance than an alteration of that authority.

In short, if the "international terrorism" requirement is taken seriously, use of the lone-wolf power runs afoul of no constitutional limitation.

The limited nature of the exception is demonstrated in a tangible sense by the fact that the government to this point has never been forced to rely upon it, instead making use of ordinary criminal-law procedures that are beyond any constitutional doubt.[26] This suggests that otherwise identical investigations that are conducted for foreign-intelligence purposes pass constitutional muster.

It would be mistaken, however, to conclude that the two are perfect substitutes and that "lone wolf" may be let to lapse. It is easy to imagine circumstances in which the ordinary procedures would be insufficient or would cause delays in investigation.

Conclusion

Notwithstanding the overblown rhetoric that seems to drown out any sensible debate about the powers authorized by the Patriot Act and subsequent legislation, the anti-terrorism authorities that Congress has declined to make permanent are not subject to serious constitutional doubt. Instead, they build modestly on the framework established by FISA and refined by three decades of practice, as well as the tools employed in ordinary criminal investigations.

Rather than a broad and ill-defined scope, each provides a specific authority to address specific lapses in authority to conduct certain foreign-intelligence investigations. As such, the primary risks presented by reauthorization are (1) that any reauthorization will be for too brief a period of time to provide adequate certainty in counterterrorism investigations and (2) that Congress will continue to treat last-minute reauthorization as an adequate substitute for routine and continuing oversight.

Unconstitutional overreaching by the federal government is a distressingly regular occurrence, but reauthorization of these tools is both legitimate and constitutional.

*—**Andrew M. Grossman** is a Visiting Legal Fellow in the Center for Legal & Judicial Studies at The Heritage Foundation.*

25. This is hypothetical, of course, because it is difficult to imagine how the government would make the requisite showing to obtain a FISA order in such circumstances.
26. *See* Rowan, *supra* note 15.