

A New Surveillance Act
By Richard A. Posner

The best, and probably the only, way to end the debate over the propriety of the National Security Agency's conducting electronic surveillance outside the framework of the Foreign Intelligence Surveillance Act is for Congress to enact a new statute.

The administration is right to point out that FISA, enacted in 1978 -- long before the danger of global terrorism was recognized and electronic surveillance was transformed by the digital revolution -- is dangerously obsolete. It retains value as a framework for monitoring the communications of known terrorists, but it is hopeless as a framework for detecting terrorists. It requires that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance is a terrorist, when the desperate need is to find out who is a terrorist.

Critics of the NSA's program point out that surveillance not cabined by a probable-cause requirement produces many false positives (intercepts that prove upon investigation to have no intelligence value). That is not a sound criticism.

National security intelligence is a search for the needle in a haystack. The intelligence services must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented. The initial trolling for clues is done by computer search programs, which do not invade privacy because search programs are not sentient beings. The programs pick out a tiny percentage of communications to be read by (human) intelligence officers, and a small subset of these will turn out to have intelligence value and spur an investigation. Some of these may be communications to which a U.S. citizen is a party.

The program is vital, given the terrorist menace, which is real and not abating. It may be thanks to such programs, as well as to other counterterrorist operations, that we have been spared a repetition of 9/11. We mustn't let our guard down, basking in the false assurance created by the lapse of time since the last attack. But the legality of the program has been called into question, and fears have been expressed about its impact on civil liberties.

These concerns can be addressed without gutting the program. But not by relaxing the standard for obtaining a warrant. Instead of requiring probable cause to believe the target a terrorist, FISA could be amended to require merely reasonable suspicion. But even that would be too restrictive. And the lower the standard for getting a warrant, the less of a filter a warrant requirement creates. If all that the government is required to state in its application is that it thinks an interception might yield intelligence information, judges will have no basis for refusing to grant the application.

* * *

It is a mistake to think that the only way to prevent abuses of a surveillance program is by requiring warrants. Congress could enact a statute that would subject warrantless electronic surveillance to tight oversight and specific legal controls, as follows:

1. Oversight: The new statute would --

(a) Create a steering committee for national security electronic surveillance composed of the attorney general, the director of national intelligence, the secretary of homeland security (chairman), and a senior or retired federal judge or justice appointed by the chief justice of the United States. The committee would monitor all such surveillance to assure compliance with the Constitution and laws.

(b) Require the NSA to submit to the FISA court, every six months, a list of the names and other identifying information of all persons whose communications had been intercepted without a warrant in the previous six months, with a brief statement of why these individuals had been targeted. If the court concluded that an interception had been inappropriate, it would so report to the steering committee and the congressional intelligence committees.

2. Specific controls: The statute would --

(a) Authorize "national security electronic surveillance" outside FISA's existing framework, provided that Congress declared a national emergency and the president certified that such surveillance was necessary in the national interest. Warrants would continue to be required for all physical searches and for all electronic surveillance for which FISA's existing probable-cause requirement could be satisfied.

(b) Define "national security" narrowly, excluding "ecoterrorism," animal-rights terrorism, and other forms of political violence that, though criminal and deplorable, do not endanger the nation.

(c) Sunset after five years, or sooner if the declaration of national emergency was rescinded.

(d) Forbid any use of intercepted information for any purpose other than "national security" as defined in the statute (point b above). Thus the information could not be used as evidence or leads in a prosecution for ordinary crime. There would be heavy criminal penalties for violating this provision, to allay concern that "wild talk" picked up by electronic surveillance would lead to criminal investigations unrelated to national security.

(e) Require responsible officials to certify to the FISA court annually that there had been no violations of the statute during the preceding year. False certification would be punishable as perjury.

(f) Bar lawsuits challenging the legality of the NSA's current warrantless surveillance program. Such lawsuits would distract officials from their important duties, to no purpose given the new statute.

Mr. Posner is a judge on the U.S. Seventh Circuit Court of Appeals and a senior lecturer in law at the University of Chicago Law School.