The New York Times

July 6, 2013

In Secret, Court Vastly Broadens Powers of N.S.A.

By ERIC LICHTBLAU

WASHINGTON — In more than a dozen classified rulings, the nation's surveillance court has created a secret body of law giving the National Security Agency the power to amass vast collections of data on Americans while pursuing not only terrorism suspects, but also people possibly involved in nuclear proliferation, espionage and cyberattacks, officials say.

The rulings, some nearly 100 pages long, reveal that the court has taken on a much more expansive role by regularly assessing broad constitutional questions and establishing important judicial precedents, with almost no public scrutiny, according to current and former officials familiar with the court's classified decisions.

The 11-member Foreign Intelligence Surveillance Court, known as the FISA court, was once mostly focused on approving case-by-case wiretapping orders. But since major changes in legislation and greater judicial oversight of intelligence operations were instituted six years ago, it has quietly become almost a parallel Supreme Court, serving as the ultimate arbiter on surveillance issues and delivering opinions that will most likely shape intelligence practices for years to come, the officials said.

Last month, a former National Security Agency contractor, Edward J. Snowden, leaked a classified order from the FISA court, which authorized the collection of all phone-tracing data from Verizon business customers. But the court's still-secret decisions go far beyond any single surveillance order, the officials said.

"We've seen a growing body of law from the court," a former intelligence official said. "What you have is a common law that develops where the court is issuing orders involving particular types of surveillance, particular types of targets."

In one of the court's most important decisions, the judges have expanded the use in terrorism cases of a legal principle known as the "special needs" doctrine and carved out an exception to the Fourth Amendment's requirement of a warrant for searches and seizures, the officials said.

The special needs doctrine was originally established in 1989 by the Supreme Court in a ruling allowing the drug testing of railway workers, finding that a minimal intrusion on privacy was justified by the government's need to combat an overriding public danger. Applying that concept more broadly, the FISA judges have ruled that the N.S.A.'s collection and examination of Americans' communications data to track possible terrorists does not run afoul of the Fourth Amendment, the officials said.

That legal interpretation is significant, several outside legal experts said, because it uses a relatively narrow area of the law — used to justify airport screenings, for instance, or drunken-driving checkpoints — and applies it much more broadly, in secret, to the wholesale collection of communications in pursuit of terrorism suspects. "It seems like a legal stretch," William C. Banks, a national security law expert at Syracuse University, said in response to a description of the decision. "It's another way of tilting the scales toward the government in its access to all this data."

While President Obama and his intelligence advisers have spoken of the surveillance programs leaked by Mr. Snowden mainly in terms of combating terrorism, the court has also interpreted the law in ways that extend into other national security concerns. In one recent case, for instance, intelligence officials were able to get access to an e-mail attachment sent within the United States because they said they were worried that the e-mail contained a schematic drawing or a diagram possibly connected to Iran's nuclear program.

In the past, that probably would have required a court warrant because the suspicious e-mail involved American communications. In this case, however, a

little-noticed provision in a 2008 law, expanding the definition of "foreign intelligence" to include "weapons of mass destruction," was used to justify access to the message.

The court's use of that language has allowed intelligence officials to get wider access to data and communications that they believe may be linked to nuclear proliferation, the officials said. They added that other secret findings had eased access to data on espionage, cyberattacks and other possible threats connected to foreign intelligence.

"The definition of 'foreign intelligence' is very broad," another former intelligence official said in an interview. "An espionage target, a nuclear proliferation target, that all falls within FISA, and the court has signed off on that."

The official, like a half-dozen other current and former national security officials, discussed the court's rulings and the general trends they have established on the condition of anonymity because they are classified. Judges on the FISA court refused to comment on the scope and volume of their decisions.

Unlike the Supreme Court, the FISA court hears from only one side in the case — the government — and its findings are almost never made public. A Court of Review is empaneled to hear appeals, but that is known to have happened only a handful of times in the court's history, and no case has ever been taken to the Supreme Court. In fact, it is not clear in all circumstances whether Internet and phone companies that are turning over the reams of data even have the right to appear before the FISA court.

Created by Congress in 1978 as a check against wiretapping abuses by the government, the court meets in a secure, nondescript room in the federal courthouse in Washington. All of the current 11 judges, who serve seven-year terms, were appointed to the special court by Chief Justice John G. Roberts Jr., and 10 of them were nominated to the bench by Republican presidents. Most hail from districts outside the capital and come in rotating shifts to hear surveillance applications; a single judge signs most surveillance orders, which totaled nearly 1,800 last year. None of the requests from the intelligence agencies was denied, according to the court.

Beyond broader legal rulings, the judges have had to resolve questions about newer types of technology, like video conferencing, and how and when the government can get access to them, the officials said.

The judges have also had to intervene repeatedly when private Internet and phone companies, which provide much of the data to the N.S.A., have raised concerns that the government is overreaching in its demands for records or when the government itself reports that it has inadvertently collected more data than was authorized, the officials said. In such cases, the court has repeatedly ordered the N.S.A. to destroy the Internet or phone data that was improperly collected, the officials said.

The officials said one central concept connects a number of the court's opinions. The judges have concluded that the mere collection of enormous volumes of "metadata" — facts like the time of phone calls and the numbers dialed, but not the content of conversations — does not violate the Fourth Amendment, as long as the government establishes a valid reason under national security regulations before taking the next step of actually examining the contents of an American's communications.

This concept is rooted partly in the "special needs" provision the court has embraced. "The basic idea is that it's O.K. to create this huge pond of data," a third official said, "but you have to establish a reason to stick your pole in the water and start fishing."

Under the new procedures passed by Congress in 2008 in the FISA Amendments Act, even the collection of metadata must be considered "relevant" to a terrorism investigation or other intelligence activities.

The court has indicated that while individual pieces of data may not appear "relevant" to a terrorism investigation, the total picture that the bits of data create may in fact be relevant, according to the officials with knowledge of the decisions.

Geoffrey R. Stone, a professor of constitutional law at the University of Chicago, said he was troubled by the idea that the court is creating a significant body of law without hearing from anyone outside the government, forgoing the

adversarial system that is a staple of the American justice system. “That whole notion is missing in this process,” he said.

The FISA judges have bristled at criticism that they are a rubber stamp for the government, occasionally speaking out to say they apply rigor in their scrutiny of government requests. Most of the surveillance operations involve the N.S.A., an eavesdropping behemoth that has listening posts around the world. Its role in gathering intelligence within the United States has grown enormously since the Sept. 11 attacks.

Soon after, President George W. Bush, under a secret wiretapping program that circumvented the FISA court, authorized the N.S.A. to collect metadata and in some cases listen in on foreign calls to or from the United States. After a heated debate, the essential elements of the Bush program were put into law by Congress in 2007, but with greater involvement by the FISA court.

Even before the leaks by Mr. Snowden, members of Congress and civil liberties advocates had been pressing for declassifying and publicly releasing court decisions, perhaps in summary form.

Reggie B. Walton, the FISA court’s presiding judge, wrote in March that he recognized the “potential benefit of better informing the public” about the court’s decisions. But, he said, there are “serious obstacles” to doing so because of the potential for misunderstanding caused by omitting classified details.

Gen. Keith B. Alexander, the N.S.A. director, was noncommital when he was pressed at a Senate hearing in June to put out some version of the court’s decisions.

While he pledged to try to make more decisions public, he said, “I don’t want to jeopardize the security of Americans by making a mistake in saying, ‘Yes, we’re going to do all that.’ ”