

The New York Times

August 21, 2013

Secret Court Rebuked N.S.A. on Surveillance

By CHARLIE SAVAGE and SCOTT SHANE

WASHINGTON — A federal judge sharply rebuked the [National Security Agency](#) in 2011 for repeatedly misleading the court that oversees its surveillance on domestic soil, including a program that is collecting tens of thousands of domestic e-mails and other Internet communications of Americans each year, according to a secret ruling made public on Wednesday.

The [85-page ruling](#) by Judge John D. Bates, then serving as chief judge on the Foreign Intelligence Surveillance Court, involved an N.S.A. program [that systematically searches the contents of Americans' international Internet communications](#), without a warrant, in a hunt for discussions about foreigners who have been targeted for surveillance.

The Justice Department had told Judge Bates that N.S.A. officials had discovered that the program had also been gathering domestic messages for three years. Judge Bates found that the agency had violated the Constitution and declared the problems part of a pattern of misrepresentation by agency officials in submissions to the secret court.

The release of the ruling, the subject of a Freedom of Information Act lawsuit, was the latest effort by the Obama administration to gain control over revelations about N.S.A. surveillance prompted by leaks by the former agency contractor Edward J. Snowden.

The collection is part of a broader program under a 2008 law that allows warrantless surveillance on domestic networks as long as it is targeted at noncitizens abroad. The purely domestic messages collected in the hunt for discussions about targeted foreigners represent a relatively small percentage of what the ruling said were 250 million communications intercepted each year in that broader program.

While the N.S.A. fixed problems with how it handled those purely domestic messages to the court's satisfaction, the 2011 ruling revealed further issues.

“The court is troubled that the government’s revelations regarding N.S.A.’s acquisition of Internet transactions mark the third instance in less than three years in which the

government has disclosed a substantial misrepresentation regarding the scope of a major collection program,” Judge Bates wrote.

One of the examples was redacted in the ruling. Another involved a separate N.S.A. program that keeps logs of all domestic phone calls, which the court approved in 2006 and which came to light in June as a result of leaks by Mr. Snowden.

In March 2009, a footnote said, the surveillance court learned that N.S.A. analysts were using the phone log database in ways that went beyond what the judges believed to be the practice because of a “repeated inaccurate statements” in government filings to the court.

“Contrary to the government’s repeated assurances, N.S.A. had been routinely running queries of the metadata using querying terms that did not meet the standard for querying,” Judge Bates recounted. He cited a 2009 ruling that concluded that the requirement had been “so frequently and systematically violated that it can fairly be said that this critical element of the overall ... regime has never functioned effectively.”

The Electronic Frontier Foundation, a free speech and privacy rights group, sued to obtain the ruling after Senator Ron Wyden, an Oregon Democrat who sits on the Senate Intelligence Committee, fought last summer to declassify the basic fact that the surveillance court had ruled that the N.S.A. had violated the Fourth Amendment.

In a statement, Mr. Wyden — an outspoken critic of N.S.A. surveillance — said declassification of the ruling was “long overdue.” He argued that while the N.S.A. had increased privacy protections for purely domestic and unrelated communications that were swept up in the surveillance, the collection itself “was a serious violation of the Fourth Amendment.”

Mark Rumold of the Electronic Frontier Foundation praised the administration for releasing the document with relatively few redactions, although he criticized the time and the difficulty in obtaining it. But he also said the ruling showed the surveillance court was not equipped to perform adequate oversight of the N.S.A.

“This opinion illustrates that the way the court is structured now it cannot serve as an effective check on the N.S.A. because it’s wholly dependent on the representations that the N.S.A. makes to it,” Mr. Rumold said. “It has no ability to investigate. And it’s clear that the N.S.A. representations have not been entirely candid to the court.”

A senior intelligence official, speaking to reporters in a conference call, portrayed the ruling as showing that N.S.A. oversight was robust and serious. He said that some 300 N.S.A.

employees were assigned to seek out even inadvertent violations of the rules and that the court conducted “vigorous” oversight.

The ruling focused on a program under which the N.S.A. has been searching domestic Internet links for communications — where at least one side is overseas — in which there are “strong selectors” indicating insider knowledge of someone who has been targeted for foreign-intelligence collection. One example would be mentioning a person’s private e-mail address in the body of an e-mail.

Most of the time, the system brings up single communications, like an e-mail or text message. But sometimes many messages are packaged and travel in a bundle that the N.S.A. calls “multi-communication transactions.”

A senior intelligence official gave one example: a Web page for a private e-mail in-box that displays subject lines for dozens of different messages — each of which is considered a separate communication, and only one of which may discuss the person who has been targeted for intelligence collection.

While Judge Bates ruled that it was acceptable for the N.S.A. to collect and store such bundled communications, he said the agency was not doing enough to minimize the purely domestic and unrelated messages to protect Americans’ privacy. In response, the N.S.A. agreed to filter out such communications and store them apart, with greater protections, and to delete them after two years instead of the usual five.

A Justice Department “white paper” released with the ruling shed new light on N.S.A. surveillance of communications streaming across domestic telecommunications networks. Such “upstream” collection, which still must be targeted at or be about noncitizens abroad, accounts for about 10 percent of all the Internet messages collected in the United States, it said; the other 90 percent are obtained from Internet companies under the system the N.S.A. calls Prism.

The administration also released a partly redacted [semiannual report](#) about “compliance” incidents, or mistakes involving the privacy rights of Americans or people in the United States. It found that there had been no willful violations of the rules, and that fewer than 1 percent of queries by analysts involved errors.

The document also showed that the government recently changed the rules to allow N.S.A. and C.I.A. analysts to search its databases of recorded calls and e-mails using search terms designed to find information involving American citizens, not foreigners — an issue that has

long concerned Senator Wyden and that was mentioned in a document leaked by Mr. Snowden and published by The Guardian.

The number of “selectors” designed to filter out and store communications targeted at foreigners had gone up steadily, the document said, although the numbers were redacted. And its increase is expected to “accelerate” because the F.B.I. recently made the ability to nominate people for such collection “more widely available to its field office personnel.”