



Guest Blogger: NSA Again Violates the Law

May 11, 2006

By Kate Martin, Director, Center for National Security Studies

Today, USA Today reported that the NSA has been secretly collecting the phone records of millions of Americans. The President held a news briefing in which he carefully failed to deny that the program exists. Such surveillance, if not authorized by the FISA court, is illegal. Depending on how it was conducted, it may also have been a crime.

Compiling a data-base of the phone calls of millions of Americans is not likely to find actual terrorists, but is a dangerous threat to the privacy and associational rights of Americans. The NSA is apparently building a database of everyone's associations, which can then be supplemented with the vast array of other information available to the government. The administration deceived the American public and the Congress about its activities when it failed to disclose this program. The existence of the program goes to the heart of the recent debates about the Patriot Act, NSA eavesdropping and data-mining.

It is illegal for the NSA to obtain records of phone numbers from the telephone companies unless the FISA court authorized it. The Stored Communications Act prohibits the telephone companies from disclosing such information to the government unless they receive a subpoena or a court order for the records. 18 U.S.C. 2702(c), 2703(c).

In the case of the NSA, the Foreign Intelligence Surveillance Court would have to issue such an order. It does not appear that it has done so, apparently because the NSA worried that it would not approve such wholesale collection of information. Moreover, if the NSA obtained such information in real time - using a pen register or trap and trace device - those who did so would be guilty of criminal conduct. (The law on pen registers and trap and trace devices provides that no one may use such a device without obtaining a court order either under the criminal wiretap law or the Foreign Intelligence Surveillance Act. 18 USC 3121.)

Some background: in 1979, the Supreme Court held that no search warrant was required for a pen register recording the numbers dialed from a particular phone number because the use of such a device was not a search under the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735 (1979). The Court's analysis that there was no reasonable expectation of privacy in the phone numbers dialed by an individual rested at least in part on the fact that the pen register obtained limited information. Whether that analysis would apply given new technological surveillance capabilities is not clear.

In all events, Congress thereafter acted to protect the privacy of such information. Just

as in the case of the bank secrecy law protecting the privacy of bank records, after the Supreme Court held that such records were not protected by the Fourth Amendment because they were held by the bank, rather than the individual, Congress required the government to obtain a court order for pen registers and trap and trace devices, 18 USC 3121 et seq., and a court order or subpoena for records of past telephone calls.

While the law provides several means for the government to obtain records showing what phone numbers were called or dialed by a particular phone number, in every instance, either a subpoena or court order is required. It appears that the NSA obtained the records of millions of Americans without having the required court order. If the NSA used a pen register or trap and trace device in real time, it was required to obtain an order from the FISA court, either under the specific pen register provisions, 50 USC 1841 et seq. or under the provisions for electronic surveillance generally, 50 USC 1801 et seq. Under the electronic surveillance provisions, the NSA would have to show the court that the person whose calls were being targeted was an agent of a foreign power. Under the pen register provision, the NSA would have to show the court that the information was relevant to an ongoing terrorism investigation. Despite the low standard for a pen register, it is unlikely that the FISA court would have approved wholesale pen registers on every phone in America. If the NSA obtained stored records, rather using a real time pen register, it would have to obtain an order from the FISA court under section 215 of the Patriot Act. That section contained an even lower standard for obtaining information.

It is important to note that the Patriot Act specifically provided that the FBI did not need a court order, but could use a National Security Letter - a form of administrative subpoena - to obtain such records. The Congress specifically withheld such subpoena authority from the NSA. The FBI investigates people or groups when it has some predication, however minimal that there is a nexus to terrorist activity. The NSA has no such limitation and thus wasn't given this broad subpoena power by the Congress. Instead the Congress required the NSA to convince the FISA court that the information would be relevant.

The President evidently decided, that he could ignore even that minimal requirement intended to insure some basic accountability by the NSA and to safeguard Americans' privacy.

UPDATE:

Since yesterday, more questions have been asked:

Could the FBI simply have obtained the same information using a National Security Letter (NSL) administrative subpoena and then shared the information with the NSA?

The short answer is no.

Some have suggested that the administration could have obtained the same information through the FBI. But this misunderstands the respective roles of the agencies and the limits on FBI and NSA activity. As the NSA would have been first to admit before its

cooptation by the White House, it did not do "domestic intelligence." That was the province of the FBI even when the intelligence concerned foreign threats. The NSA had strict rules protecting information about Americans that it came across, and more fundamentally did not aim its giant satellites and computers at domestic phone and e-mail traffic. The threat to Americans' privacy from the unselective and enormous computing power of the NSA was too great.

The FBI on the other hand, operates with greater transparency, reports to the Attorney General, not the intelligence czar or the Secretary of Defense, and conducts specific targeted foreign intelligence investigations. As FBI officials repeatedly stress, their terrorism and foreign intelligence investigations start from known facts and look at individual potential suspects. (Which is not to say that they do not do data-mining, but it begins from a different premise.) The Attorney General issues rules governing those investigations. Again, while those rules are weaker than they should be, they do presume targeted investigations; not in the words of General Hayden the "driftnet" over Americans' phone calls described by USA today.

Accordingly, when Congress gave the FBI the power to issue an NSL administrative subpoena for telephone records in an intelligence investigation, it did not give the FBI the authority to subpoena all records on everyone. When Congress first provided for secret FBI counterintelligence access to stored telephone records in 1986, it limited its access to records concerning a suspected spy or terrorist, i.e., an "agent of a foreign power" under the FISA. Congress broadened the reach of that NSL power in the Patriot Act in 2001 when it deleted the required nexus to a suspected spy or terrorist, and allowed the FBI secret access to telephone records "relevant to an authorized investigation to protect against international terrorism." 18 USC 2709 (as amended by section 505 of the Patriot Act.). While that amendment has been criticized by all of us in the civil liberties community, it was not without any limit at all. In restricting seizures of records to those relevant to an authorized investigation, Congress incorporated the Attorney General rules as well as its understanding about how FBI investigations proceed.

FBI officials over the years have repeatedly told me that they do not simply collect all data on Americans and would not do so. While they may well collect more data than they should, only unprecedented White House orders could result in the FBI attempting to use its NSL authority to obtain all the phone records that the NSA has now collected. And certainly Congress has never authorized such collection by the FBI.

Could the FISA Court properly issue an order authorizing the NSA to obtain all these records?

We don't know if the FISA court issued an order, although it seems doubtful. Unlike the telephone calls with Al Qaeda for which a FISA warrant could probably have been obtained, it is not at all clear that the FISA court could properly authorize seizure of all the phone records of all Americans.

In my post yesterday (above), I suggested that the NSA could have sought an order

under section 215 of the Patriot Act regarding business records. Upon reflection, I'm not so sure. Given the detailed statutory scheme protecting telephone records, including the pen register laws, the Stored Communications Act and FISA, it would make little sense to conclude that Congress meant to enact a broad override to those protections in section 215. While that section requires a FISA court order, before the recent Patriot Act reauthorization, it contained an almost meaningless standard for issuing that order. The better reading of the law would be to require the NSA to obtain an order under either the pen register or electronic surveillance provisions of the FISA. In neither event, is it likely that they could have obtained an order authorizing seizure of all the phone records of all Americans.