

New York Times May 12, 2006

NSA's data mining explained

By Declan McCullagh and Anne Broache

A correction was made to this story. Read below for details.

Capitol Hill politicians reacted angrily this week to a new report about how the National Security Agency is involved in not merely surveillance of phone calls, but also an extensive data mining program.

"We need to know what our government is doing in its activities that spy upon Americans," said Sen. Patrick Leahy, a Vermont Democrat. Republican Sen. Arlen Specter of Pennsylvania vowed to hold hearings to get to the bottom of how the NSA's data mining works and whether Americans' privacy rights were affected.

To answer some questions about the program and how it likely works, CNET News.com has created the following list of answers to frequently asked questions. Keep reading.

Q: What new information came out this week?

USA Today published an article on Thursday that said AT&T, Verizon and BellSouth turned over records of millions of phone calls to the National Security Agency. These are not international calls--they're apparently records of all calls that those companies' customers made.

Two things are worth noting. First, based on the newspaper's description, contents of phone calls were not divulged. Second, customers' names, street addresses and other personal information were not handed over.

Q: When you say records of phone calls were turned over, what does that mean?

That's a reference to "call detail records," or CDRs, which are database entries that record the parties to the conversation, the duration of the call and so on. This appears to include local phone calls and not just long-distance calls.

CDRs are stored in massive telephone company databases. Cisco Systems' Unified CallManager lets customers use SQL queries to dig up information about each call. Those internal databases have either been opened up to outside queries from the NSA or (more likely) duplicated and handed over to the NSA on a regular basis.

Q: If the NSA has my phone number, can it get my name and address?

Yes. The NSA can cross-check other databases to obtain that information. Many commercial data vendors, such as Yahoo People Search and LexisNexis' People Locator, do just that--and count many federal agencies among their customers.

Q: How about cell phones?

It would be a bit more difficult. There's no central directory for cell phones, for instance. And there's not much information that can be gleaned about owners of disposable cell phones who happened to buy them with cash.

Q: How is this different from what we knew before?

A series of disclosures, starting with The New York Times' report in December, outlined how the NSA conducted surreptitious electronic surveillance of phone calls and e-mail traffic when one party was outside the United States.

The president and other members of his administration have stuck to that claim--saying that domestic phone calls were not part of the dragnet. In January, for instance, Bush assured Americans that "one end of the communication must be outside the United States."

The latest revelation is different. It says the scope of the NSA's efforts is far broader than listening in on a few hundred conversations. Instead, the vast majority of Americans have probably had information on their phone calls turned over. (Another difference is that the contents of the conversations was not divulged, at least as far as we know.)

Q: When Attorney General Alberto Gonzales was testifying a few months ago, he seemed careful to specify that he was talking only about the "Terrorist Surveillance Program." Does that mean he knew about the phone data mining effort and refused to reveal it earlier?

It seems likely, but we don't know. During his appearance before the Senate Judiciary Committee and in a subsequent letter to senators, Gonzales' careful wording seemed to imply that there may be additional domestic surveillance programs beyond the one revealed by The New York Times. (Testifying before senators, Gonzales referred to that program as "the program that the president has confirmed.")

But Gonzales later reassured concerned politicians that the administration is not currently conducting any additional domestic surveillance programs, Rep. Jane Harman, the senior Democrat on the House Intelligence Committee, told The Washington Post in a March interview. Of course, Gonzales could have been parsing his words carefully--and might eventually claim that data mining is not surveillance.

Q: Now that the NSA has this mountain of data, what is the agency doing with it?

The two-word summary: data mining. That's a loose term that generally means directing a computer program to sift through large amounts of data in hopes of extracting previously unknown information.

In theory, useful patterns can emerge and future terrorist plots could be thwarted. In practice, though, The New York Times has reported that FBI sources say many of the tips provided by the NSA led to dead ends.

Q: What other data mining efforts has the NSA been involved with?

Details are classified, of course. But a few hints have become public, and we know that the NSA has funded or been otherwise involved in dozens of programs in the past.

Correction: This story mistakenly identified Sen. Bill Nelson as a Florida Republican. He is a Democrat. The New York Times reported in February that NSA officials had recently met with Silicon Valley companies while shopping for better data mining techniques.

Virage, in San Mateo, Calif., boasts that its products that can transcribe the text of audio conversations are perfect for "intelligence agencies" and lists federal agencies (including the NSA's parent agency) as customers. Another product, called Analyst's Notebook and made by the Virginia-based company i2, is in use by the FBI and many "defense and intelligence agencies."

A patent (#5,937,422) granted to the NSA in August 1999 talks about extracting topics from computer-generated text, which would include telephone conversations.

Q: Which companies are cooperating with the NSA?

We don't know the whole list. So far AT&T, Verizon and BellSouth have been named as cooperating, and Qwest has said it refused to divulge information without a court order. Cox Communications has said it was not asked to hand over anything to the NSA.

There are two odd discrepancies. A survey that we published in February asked telecommunications carriers whether they "turned over information or opened up their networks to the NSA without being compelled by law." Neither Verizon nor AT&T would give a yes or a no answer to that question.

But BellSouth did answer in the negative at the time.

Q: What's BellSouth's explanation now?

A BellSouth representative said Thursday that he could not explain the discrepancy, and provided us with a statement saying: "BellSouth does not provide any confidential customer information to the NSA or any governmental agency without proper legal authority."

The statement did not elaborate on what "proper legal authority" might be--leaving open the possibility that it includes a mere polite request from the FBI or the White House.

Q: Wait--you mentioned two odd discrepancies. What's the second?

That would be Yahoo. Under cross-examination by a House committee in February, Yahoo General Counsel Michael Callahan declined five times to say whether the company opens its records to the NSA without a court order.

Q: Is this type of data mining legal under federal law? And permissible under the Fourth Amendment to the U.S. Constitution?

It depends on who you talk to. The same people who viewed the earlier wiretapping scheme as permissible are likely to argue that data mining is also perfectly OK.

Peter Swire, who worked in the Clinton White House and now teaches privacy law, has written a set of legal FAQs that say the wiretapping was unlawful. John Eastman, a conservative law professor at the Claremont Institute, argues in a letter to Congress (click here for PDF) that the wiretapping was permissible.

As for the data mining, Jim Harper of the free-market Cato Institute says it violates the Fourth Amendment's prohibition on unreasonable searches. Orin Kerr, a former Justice Department prosecutor who takes a more permissive view of police power, says his tentative conclusion is that it does not run afoul of the Fourth Amendment but the phone companies likely violated the Stored Communications Act.

Q: What Republicans have publicly criticized the NSA spying program?

The loudest outcry has come from Sen. Arlen Specter, a moderate Pennsylvania Republican who chairs the Judiciary Committee. Specter said late last month that he was prepared to yank federal funding for the program unless the Bush Administration supplies his committee with enough information to determine whether it's legal.

New Mexico Rep. Heather Wilson, who serves on the U.S. House of Representatives Intelligence Committee, was among the first Republicans to voice her concerns about the program publicly and to call for a deeper inquiry.

Q: What has Sen. Specter done so far in response to the program?

In addition to convening four Judiciary Committee hearings aimed at vetting the program, Specter has made a public display of his skepticism about the wiretapping's constitutionality. He has repeatedly chided the Bush administration for failing to provide the necessary details that senators need to determine the program's propriety and has threatened to withhold funding for it.

He is also pushing a piece of legislation that would force the attorney general to take any existing electronic surveillance program back to the FISA court for scrutiny.

Q: What lawsuits have been filed in response to the NSA surveillance program?

Soon after the program's existence came to light, the American Civil Liberties Union sued the NSA directly in a Michigan federal court. The complaint, filed on behalf of "a diverse group of prominent journalists, scholars, attorneys and national nonprofit organizations who frequently communicate by telephone and e-mail with people outside the United States," asks that the secret wiretaps be declared unconstitutional.

The Electronic Frontier Foundation followed later in January with its own class-action suit against AT&T, alleging that the telecommunications giant opened up its facilities to the NSA in violation of the Constitution and federal wiretapping law.

But if the U.S. government gets its way, the court action won't proceed. Late last month, the Justice Department filed a document registering its intent to assert the "military and state secrets privilege" after EFF revealed it has uncovered potentially confidential documents describing a "dragnet" scheme by AT&T.

One lawsuit has already effectively ended. The Electronic Privacy Information Center sued the Justice Department in January for allegedly refusing to turn over documents related to the surveillance program in response to a Freedom of Information Act request. A federal judge ultimately ordered the government to turn over the documents by a prescribed deadline.

Q: What do Americans think of this?

According to the latest surveys, most people don't seem to mind. An ABC News-Washington Post poll published Friday found that 63 percent of the 502 random Americans surveyed found the NSA's collection of phone call records either "strongly" or "somewhat acceptable."

In that same survey, 66 percent of the respondents said it wouldn't bother them if the NSA had possession of their call logs. At the same time, just a narrow majority--51 percent--said they approved of the way President Bush has handled privacy concerns as the government investigates terrorism.

Q: What's going to happen next in Congress?

In the short term, more hearings are likely. Sen. Specter has already said he plans to call in executives from the telecommunications companies reportedly involved in the NSA program. Sen. Bill Nelson of Florida has asked the chairman of the Senate Commerce Committee to hold hearings.

House Democrats introduced a bill Thursday called the Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA, or the Listen Act. It says that covert attempts to spy on Americans or collect telephone and e-mail records must be approved by a court created by the Foreign Intelligence Surveillance Act.

Q: But haven't Democrats introduced bills before without any success?

Yes. Especially in the House of Representatives, the Republican majority enjoys a near-absolute ability to set the agenda. A number of other bills dealing with the surveillance program have been introduced but have been stuck in committee.

A mostly Democratic-backed House proposal, for instance, called the NSA Oversight Act would obligate the president to issue a classified report on how many Americans have been the subject of electronic surveillance under the NSA program.

A bill introduced by Sen. Specter would explicitly require the government to receive approval of present and future electronic surveillance programs from the Foreign Intelligence Surveillance Court.

Another bill, introduced by New York Sen. Charles Schumer, a Democrat, proposes awarding court relief to citizens who can provide evidence that they've refrained from electronic communications because of a "reasonable fear" they will be tapped.

Can the NSA conduct wiretaps without explicitly asking for phone records?

Yes. It's hardly a secret that the NSA specializes in electronic surveillance, called communications intelligence in the vernacular of spies. Author James Bamford's 1982 book "The Puzzle Palace" documented how the NSA created hundreds of "intercept stations"--ultrasophisticated, hypersensitive radio receivers designed to pluck both military signals and civilian telephone calls out of the air.

CNET News.com published an analysis in February of how the NSA does its job today. Also, an article by Bamford in last month's Atlantic Monthly recounts how the NSA has built listening posts to intercept and listen to satellite transmissions of phone calls, e-mails and other communications that travel from other countries into the United States.

The NSA has also bugged undersea fiber optic cables that link the communications in the U.S. with countries overseas. And with the permission of the phone companies, the agency has also attached monitoring equipment inside these telephone facilities so that information can be sent to NSA's supercomputers in Fort Meade, Md., to be analyzed, the article said.

Q: What about Internet communications, such as Internet telephony or e-mail messages?

Much of the Internet traffic that's transmitted in the United States traverses just a handful of switching centers owned by big communications companies, such as Verizon. The busiest are MAE East (Metropolitan Area Exchange), in Vienna, Va., and MAE West, in San Jose, Calif. The NSA has access to those switching centers, Bamford says.

In addition, the Federal Communications Commission has ordered broadband providers to build in back doors for electronic eavesdropping. A federal appeals court in Washington, D.C., heard arguments last week in a lawsuit challenging those rules.

CNET News.com's Marguerite Reardon contributed to this report.