What you should know about NSA phone data program

June 6 2013, by Matt Apuzzo

A sign stands outside the National Security Administration (NSA) campus in Fort Meade, Md., Thursday, June 6, 2013. The Obama administration on Thursday defended the National Security Agency's need to collect telephone records of U.S. citizens, calling such information "a critical tool in protecting the nation from terrorist threats." (AP Photo/Patrick Semansky)

A leaked document disclosed the monumental scale of the U.S. government's surveillance of America's phone records, part of a massive data collection program aimed at combating terrorism.

Here are some important details about the secret program and how it works:

___

Q: What happened and why is it a big deal?

A: The Guardian newspaper published a highly classified April U.S. court order that allows the government access to all of Verizon's phone records on a daily basis, for both domestic and international calls. That doesn't mean the government is listening in, and the National Security Agency did not receive the names and addresses of customers. But it did receive all phone numbers with outgoing or incoming calls, as well as the unique electronic numbers that identify cellphones. That means the government knows which phones are being used, even if customers change their numbers.

This is the first tangible evidence of the scope of a domestic surveillance program that has existed for years but has been discussed only in generalities. It proves that, in the name of national security, the government sweeps up the call records of Americans who have no known ties to terrorists or criminals.

___

Q: How is this different from the NSA wiretapping that was going on under President George W. Bush?

A: In 2005, The New York Times revealed that Bush had signed a secret order allowing the NSA to eavesdrop on Americans without court approval, a seismic shift in policy for an agency that had previously been prohibited from spying domestically. The exact scope of that program has never been known, but it allowed the NSA to monitor phone calls

and emails. After it became public, the Bush administration dubbed it the "Terrorist Surveillance Program" and said it was a critical tool in protecting the United States from attack.

"The NSA program is narrowly focused, aimed only at international calls and targeted at al-Qaida and related groups," the Justice Department said at the time.

But while wiretapping got all the attention, the government was also collecting call logs from American phone companies as part of that program, a U.S. official said Thursday. After the wiretapping controversy, the collection of call records continued, albeit with court approval. That's what we're seeing in the newly released court document: a judge's authorization for something that began years ago with no court oversight.

___

Q: Why does the government even want my phone records?

A: They're not interested in your records, in all likelihood, but your calls make up the background noise of the global phone system.

Look at your monthly phone bill, and you'll see patterns: calls home as you leave work, food delivery orders on Friday nights, that once-a-week call to mom and dad.

It's like that, except on a monumentally bigger scale.

The classified court ruling doesn't say what the NSA intends to do with your records. But armed with the nation's phone logs, the agency's computers have the ability to identify what normal call behavior looks like. And, with powerful computers, it would be possible to compare the

entire database against computer models the government believes show what terrorist calling patterns look like.

Further analysis could identify what are known in intelligence circles as "communities of interest"—the networks of people who are in contact with targets or suspicious phone numbers.

Over time, the records also become a valuable archive. When officials discover a new phone number linked to a suspected terrorist, they can consult the records to see who called that number in the preceding months or years.

Once the government has narrowed its focus on phone numbers it believes are tied to terrorism or foreign governments, it can go back to the court with a wiretap request. That allows the government to monitor the calls in real time, record them and store them indefinitely.

___

Q: Why just Verizon?

A: It's probably not. A former U.S. intelligence official familiar with the NSA program says that records from all U.S. phone companies would be seized, and that they would include business and residential numbers. Only the court order involving Verizon has been made public.

In 2006, USA Today reported that the NSA was secretly collecting the phone call records of tens of millions of Americans. The newspaper identified phone companies that cooperated in that effort. The newspaper ultimately distanced itself from that report after some phone companies denied being part of such a government program.

The court document published by The Guardian, however, offers

credence to the original USA Today story, which declared: "The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans—most of whom aren't suspected of any crime."

This undated US government photo shows an aerial view of the National Security Agency (NSA) in Fort Meade, Md. The Obama administration on Thursday defended the National Security Agency's need to collect telephone records of U.S. citizens, calling such information "a critical tool in protecting the nation from terrorist threats." (AP Photo/US Government)

Q: But in this case, a judge approved it. Does that mean someone had to show probable cause that a crime was being committed?

A: No. The seizure was authorized by the Foreign Intelligence Surveillance Court, which operates under very different rules from a typical court. Probable cause is not required.

The court was created by the Foreign Intelligence Surveillance Act of 1978 and is known in intelligence circles as the FISA court. Judges appointed by the president hear secret evidence and authorize wiretapping, search warrants and other clandestine efforts to monitor suspected or known spies and terrorists.

For decades, the court was located in a secure area at Justice Department headquarters. While prosecutors in criminal cases must come to court seeking subpoenas, the FISA judges came to the Justice Department. That changed in 2008 with the construction of a new FISA court inside the U.S. District Court in Washington. The courtroom is essentially a vault, designed to prevent anyone from eavesdropping on what goes on inside.

In this instance, Judge Roger Vinson authorized the NSA to seize the phone records under a provision in the USA Patriot Act, which passed shortly after the Sept. 11, 2001, attacks and vastly expanded the government's ability to collect information on Americans.

___

Q: If not probable cause, what standard did the government use in this case?

A: The judge relied on one of the most controversial aspects of the Patriot Act: Section 215, which became known colloquially as the "library records provision" because it allowed the government to seize a wide range of documents, including library records. Under that provision, the government must show that there are "reasonable grounds

to believe" that the records are relevant to an investigation intended to "protect against international terrorism or clandestine intelligence activities."

Exactly what "relevant" meant has been unclear. With the release of the classified court order, the public can see for the first time that everyone's phone records are relevant.

The Justice Department has staunchly defended Section 215, saying it was narrowly written and has safeguarded liberties.

Some in Congress, however, have been sounding alarms about it for years. Though they are prohibited from revealing what they know about the surveillance programs, Democratic Sens. Ron Wyden of Oregon and Mark Udall or Colorado have said the government's interpretation of the law has gone far beyond what the public believes.

"We believe most Americans would be stunned to learn the details of how these secret court opinions have interpreted section 215 of the Patriot Act," the senators wrote in a letter to Attorney General Eric Holder last year.

___

Q: Why don't others in Congress seem that upset about all this?

A: Many members of Congress have known this was going on for years. While Americans might be surprised to see, in writing, an authorization to sweep up their phone records, that's old news to many in Congress.

"Everyone should just calm down and understand that this isn't anything that's brand new," Senate Majority Leader Harry Reid said Thursday. "It's been going on for some seven years."

Senate Intelligence Committee Chairman Dianne Feinstein and Vice Chairman Saxby Chambliss issued a similar statement:

"The executive branch's use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress."

___

Q: What does the Obama administration have to say about this?

A: So far, very little. Despite campaigning against Bush's counterterrorism efforts, President Barack Obama has continued many of the most controversial ones including, it is now clear, widespread monitoring of American phone records.

The NSA is particularly reluctant to discuss its programs. Even as it has secretly collected millions of phone records, it has tried to cultivate an image that it was not in the domestic surveillance business.

In March, for instance, NSA spokeswoman Vanee Vines, emailed an Associated Press reporter about a story that described the NSA as a monitor of worldwide internet data and phone calls.

"NSA collects, monitors, and analyzes a variety of (asterisk)(asterisk)(asterisk)FOREIGN(asterisk)(asterisk)(asterisk) signals and communications for indications of threats to the United States and for information of value to the U.S. government," she wrote. "(asterisk)(asterisk)(asterisk)FOREIGN(asterisk)(asterisk)(asterisk) is the operative word. NSA is not an indiscriminate vacuum, collecting anything and everything."

—

Q: Why hasn't anyone sued over this?

A: People have sued. But challenging the legality of secret wiretaps is difficult because, in order to sue, you have to know you've been wiretapped. In 2006, for instance, a federal judge in Detroit declared the NSA warrantless wiretapping program unconstitutional. But the ruling was overturned when an appeals court that said the plaintiffs—civil rights groups, lawyers and scholars—didn't have the authority to sue because they couldn't prove they were wiretapped.

Court challenges have also run up against the government's ability to torpedo lawsuits that could jeopardize state secrets.

The recent release of the classified court document is sure to trigger a new lawsuit in the name of Verizon customers whose records were seized. But now that the surveillance program is under the supervision of the FISA court and a warrant was issued, a court challenge is more difficult.

Suing Verizon would also be difficult. A lawsuit against AT&T failed because Congress granted telecommunications companies retroactive immunity for cooperating with warrantless surveillance. In this instance, Verizon was under a court order to provide the records to the government, making a lawsuit against the company challenging.

—

Q: Can the government read emails?

A: Not under this court order, but it's not clear whether the NSA is monitoring email content as part of this program.

In 2006, former AT&T technician Mark Klein described in federal court papers how a "splitter" device in San Francisco siphoned millions of Americans' Internet traffic to the NSA. That probably included data sent to or from AT&T Internet subscribers, such as emails and the websites they visited.

Most email messages are sent through the Internet in "plain-text" form, meaning they aren't encrypted and anyone with the right tools can view their contents. Similar to an old-fashioned envelope and letter, every email contains details about whom it's from and where it's supposed to go.

Unlike postal letters, those details can include information that can be linked to a subscriber's billing account, even if he or she wants to remain anonymous.

In May 2012, Wyden and Udall asked the NSA how many people inside the United States had their communications "collected or reviewed."

The intelligence community's inspector general, I. Charles McCullough III, told the senators that providing such an estimate "would likely impede the NSA's mission" and "violate the privacy of U.S. persons."