But wait, there's more: A US spying Q&A

June 7 2013, by Matt Apuzzo

An aerial view of the NSA's Utah Data Center in Bluffdale, Utah, Thursday, June 6, 2013. The government is secretly collecting the telephone records of millions of U.S. customers of Verizon under a top-secret court order, according to the chairwoman of the Senate Intelligence Committee. The Obama administration is defending the National Security Agency's need to collect such records, but critics are calling it a huge over-reach. (AP Photo/Rick Bowmer)

Wait, there's more? Yes, this was the week that America's intelligence secrets spilled out: Classified court orders. Top secret Power Point slides. Something called PRISM. It's pretty important stuff, once you've made sense of it.

Here's what you need to know.

___

Q: The past two days have been packed with coverage about domestic surveillance. I have no idea what I'm hearing.

A: That's not a question. So let's start from the beginning, which in the national security world these days means going back to 9/11.

Shortly after the attacks, Congress hastily approved the USA Patriot Act. That gave the government wide new powers to collect information on Americans. In the first few years, news coverage focused on how the FBI would use these new powers to seize phone, bank and library records.

Separate from the Patriot Act, though, President George W. Bush authorized the National Security Agency to conduct a highly classified wiretapping program. Normally, the government needs a warrant to spy on Americans, but Bush allowed the NSA to eavesdrop on U.S. citizens, read their emails and collect their phone records—all without warrants.

In 2005, The New York Times revealed the existence of that program. Amid the furor, the rules changed. The wiretapping operation and the collection of phone records could continue, but a judge had to sign off on them.

The scope of those programs wasn't fully known. But the government assured people that the spying was narrow and kept them safe. Congress voted to continue the authority.

Then this week, The Guardian newspaper published a classified court document from April that authorized the government to seize all of

Verizon's phone records on a daily basis—an estimated 3 billion phone calls a day. The government didn't eavesdrop on anyone (under this court order, at least), but it received all outgoing and incoming numbers for every call, plus the unique electronic fingerprints that identify cellphones.

A program that the government said was narrow was suddenly revealed as vast. Under Bush and then President Barack Obama, the National Security Agency had built a colossal database of American phone calls.

___

Q: That's a lot to digest. Is that it?

A: Nope. A day after the court document surfaced, the Guardian and The Washington Post published stories and secret Power Point slides revealing another classified spying program. Unlike the effort to collect phone records, this one hadn't even been hinted about publicly.

This program, code-named PRISM, allowed the NSA and FBI to tap directly into the servers of major U.S. Internet companies such as Google, Apple, Microsoft, Facebook and AOL.

Like the phone-records program, PRISM was approved by a judge in a secret court order. Unlike that program, however, PRISM allowed the government to seize actual conversations: emails, video chats, instant messages and more.

___

Q: How does that work?

A: You're going to hear a lot about PRISM and, when you do it's

important to remember two things:

First, it's no less than astonishing that reporters obtained such highly classified, detailed documents about an ongoing intelligence-gathering program.

Second, for all the incredible details, we still know relatively little about the program. The slides appear to be from an internal NSA presentation explaining the value of PRISM to analysts. So they don't get very technical and they leave a lot unanswered.

Imagine someone trying to understand the way a company works using only the slides from the most recent staff meeting. That's what this is.

From the documents, it's clear that the NSA receives data directly from the Internet companies. The information varies by company but includes emails, your social networking activity, the files you receive, even family photos.

___

Q: What do they do with that stuff?

A: It's not clear from the documents but, as with phone records, the NSA appears to be building a database of much of the Internet traffic.

The companies participating in PRISM produce enormous amounts of data every day, so storing it would require computing power the likes of which the public has never seen. People who study technology and security believe that's why the NSA has been building a million-square-foot data center near Salt Lake City.

That center will reportedly cost about $2 billion to construct—and $40

million a year to power such a wide swath of supercomputers.

Forget megabytes, gigabytes and terabytes. According to a report last year by Wired magazine, the Utah facility will be able to handle so much information that its storage capacity is measured in what are known as yottabytes. A yottabyte is so big as to be nearly unimaginable by casual computer users: It's enough information to fill 200 trillion DVDs.

It's more information than moves through the entire Internet in a single year.

Computer scientists don't have a name for whatever is bigger than a yottabyte. It's so big, they don't need one yet.

___

Q: Does this apply to Americans?

A: Yes, definitely.

___

Q: But Obama said Friday that Americans are not targeted by this program.

A: That's also, true. It all comes down to the word "targeted." Here's why.

The agency can't target Americans. But targeting is different from collecting. PRISM dumps massive amounts of data from users all over the world into the NSA's computers, and much of that comes from the accounts of American citizens.

All this information lives on NSA computer servers. At this point, the government has your information but can still say it hasn't targeted you. Basically, PRISM might have all your emails but, until someone reads them, you haven't been targeted.

NSA analysts are supposed to focus only on non-U.S. citizens outside the United States. According to the Post, though, "incidental" collection of Americans' data is common, even at the targeting stage.

Let's say analysts are looking at a suspected terrorist. They pull his emails and all his Facebook friends. Then they take all those people and pull their data, too.

According to NSA training materials obtained by the Post, analysts are required to report to their superiors whenever this results in collection of U.S. content, but, the training materials say, "it's nothing to worry about."

___

Q: How is this legal?

A: Again, the PRISM documents don't spell out the whole program. James Clapper, the director of national intelligence, said late Thursday that it was approved by a judge and is conducted in accordance with U.S. law.

Because the authorization came from the Foreign Intelligence Surveillance Court, all the legal justification is classified.

That court was created by the Foreign Intelligence Surveillance Act of 1978 and is known in intelligence circles as the FISA court. Cases are heard inside vaults in a Washington federal courthouse. Its rulings are

almost never made public.

It's not clear whether the companies agreed to be part of PRISM voluntarily or were under court order but, either way, the companies almost certainly signed agreements with the government spelling out their cooperation. The Post reported that the government has the authority to force companies to participate.

___

Q: But the companies are denying all this, right?

A: Sort of.

Apple, for instance, issued a statement saying it had "never heard of PRISM."

That's not surprising. PRISM is a government codename for a collection effort known officially as US-984XN. There would be no reason for the NSA to share the code name with the companies.

Apple's statement continued, "We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order."

From what we know about PRISM, there apparently was a FISA court order authorizing this effort. And PRISM does not require direct access to company servers. More likely, in fact, the NSA or the companies would set up a designated route to transfer data to the government. That's easier for the company and less legally problematic for the NSA.

Other companies issued similar statements that don't necessarily preclude their involvement in PRISM. But certainly they raise more

questions about what, exactly, was going on. And the companies' statements are another reminder that we still don't know much about how PRISM worked.

___

Q: Just last week we were talking about how the administration seized the phone records from the AP and Fox News. Was that part of this program?

A: No. Surveillance authorized by the FISA court can be used only to gather intelligence. It isn't supposed to be used for law enforcement.

In the cases mentioned, the Justice Department is investigating who provided the news organizations with classified information. It's part of Obama's crackdown on officials who speak to journalists without the government's blessing. Since the goal is to bring criminal charges against someone, the Justice Department seized records using run-of-the-mill court orders.

___

Q: Is this newly detailed surveillance keeping America safe?

A: The Obama administration, like the Bush administration before it, says yes. But because both the phone data program and PRISM remain classified, it's impossible to thoroughly verify these claims.

The president can choose what he wants to declassify, which gives him an advantage in the debate for public opinion. And the politics of national security are stark: Terrorist threats tend to raise demand for new, more aggressive surveillance tactics; the absence of attacks helps justify the surveillance.

The documents obtained by the Post and Guardian show that PRISM has been a major source of intelligence, one that provides more information to the president's morning briefing book than any other program.

Obama said Friday that Congress was well aware of these programs and a FISA judge approved them.

___

Q: So what's the scandal here?

A: This week, Americans have gotten a glimpse at a government surveillance machine that has been churning for years, gathering information on its citizens.

The stories are important not because they show rogue, illegal government spying. They matter because they reveal, in stark fashion, what the government has made legal over the past decade and where that has taken the country.