Written by **Jack Kenny** on June 8, 2013

Obama Defends Mass Surveillance; Internet Firms Deny Playing Part

"Nobody is listening to the content of people's phone calls," President Obama said Friday as he sought to allay concern arising from news reports over the previous two days of massive data gathering of telephone records, e-mail messages, and other communications by the National Security Agency. Saying he didn't want the day to "just be a bleeding press conference," the president took two questions from reporters in San Jose, California, following his speech on the Affordable Care Act.

"Mr. President," asked Jackie Calmes of the *New York Times*, "could you please react to the reports of secret government surveillance of phones and Internet? And can you also assure Americans that the government — your government — doesn't have some massive secret database of all their personal online information and activities?"

The president began by citing congressional support for the surveillance programs, noting that "relevant intelligence committees have been briefed on these programs. These are programs that have been authorized by broad bipartisan majorities repeatedly since 2006." He also insisted that the right of privacy is reasonably protected by procedural safeguards in the programs.

The programs "make a difference in our capacity to anticipate and prevent possible terrorist activity," Obama said, adding that they are "under very strict supervision by all three branches of government and they do not involve listening to people's phone calls, do not involve reading the e-mails of U.S. citizens and U.S. residents."

"As was indicated, what the intelligence community is doing is looking at phone numbers and durations of calls," Obama continued. "They are not looking at people's names, and they're not looking at content." Before members of the "intelligence community" may listen to a phone call, he said, "they've got to go back to a federal judge, just like they would in a criminal investigation."

But in the case of a warrant such as the April 25 Foreign Intelligence Surveillance Court order, authorizing the collection of all of Verizon's call logs every day for three months, the judge that the FBI or NSA goes back to is not an impartial magistrate. The court was created by the Foreign Intelligence Surveillance Act of 1978 and is often referred to as the FISA court. It is located in the headquarters building of the Department of Justice, the prosecutorial arm of the federal government. It almost never turns down a request for a warrant and rarely modifies one. It is easy enough for intelligence analysts to find the name that goes with any phone number, making the president's statement that intelligence analysts are looking only at numbers, not names, essentially meaningless. And it is easy enough to get a warrant when they want to listen to phone calls.

"This is a court that meets in secret, allows only the government to appear before it, and publishes almost none of its opinions," Jameel Jaffer, deputy director of the American Civil Liberties Union, said to

the *Washington Post*. "It has never been an effective check on government."

Obama, who was an outspoken critic of surveillance activities by the George W. Bush administration, acknowledged that he took office with "a healthy skepticism about some of these programs," but came to realize they were needed. "We've scrubbed them thoroughly," he said, and expanded safeguard and oversight provisions. "And if there are members of Congress who feel differently, then they should speak up. And we're happy to have that debate," he stated.

But members of Congress who have been briefed on classified information are forbidden by law to divulge what they've learned. In letters to Attorney General Eric Holder on in 2011 and again last year, U.S. Senators Ron Wyden of Oregon and Mark Udall of Colorado, both Democrats, protested the secrecy surrounding interpretations by the FISA court of the government's power under the business records section of the Patriot Act. Even the interpretations are classified, they wrote, making public debate about them all but impossible.

"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 said in their March 15, 2012 letter to Holder. "As we see it, there is now a significant gap between what most Americans *think* the law allows and what the government *secretly claims* the law allows." (Emphasis in original.)

The court orders themselves come with a gag rule forbidding those served with warrants from disclosing the orders to anyone other than an attorney for the purpose of helping them comply. Perhaps that's why some of the Internet companies named in the *Washington Post* story on the PRISM program issued carefully worded and remarkably similar statements denying participation in a massive data-gathering program by the National Security Agency.

"We have never heard of PRISM," said Steve Dowling, a spokesman for Apple. "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."

"We do not provide any government organization with direct access to Facebook servers," said Joe Sullivan, chief security officer for Facebook. "When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law."

But that can be quite extensive, indeed, as is evident in the FISA court's order to Verizon. Google issued a statement saying, "We have not joined any program that would give the U.S. government — or any other government — direct access to our servers. Indeed, the U.S. government does not have direct access or a "back door" to the information stored in our data centers. We had not heard of a program called PRISM until yesterday."

Yahoo also released a statement saying it does not "provide the government with direct access" to its servers. And Microsoft said: "We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis."

Well, there's nothing voluntary about complying with a court order, especially one issued by a secret tribunal that a former NSA intelligence analyst called "a kangaroo court with a rubber stamp." And the companies' statements, so similar they appear to have been coordinated, all speak of the government having no "direct access" to their servers. Might there be "indirect" access, despite Google's denial of any "back door" open to the government?

In their 2010 series in the *Washington Post* called "Top Secret America," Dana Priest and William Arkin wrote: "Every day collections systems at the National Security Agency intercept and store 1.7 billion e-mails, phone calls and other types of communications." That's a whole lot of access, however obtained, through however many back, front, or side doors.

Director of National Intelligence James Clapper late Thursday night called the leaks of classified documents about the NSA data gathering through the PRISM program "reprehensible" and said the disclosure of the court order authorizing the collection of the Verizon records will be damaging to national security.

"The unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation," Clapper said. Obama, in his remarks Friday morning, made the same point.

"If every step that we're taking to try to prevent a terrorist act is on the front page of the newspapers or on television, then presumably the people who are trying to do us harm are going to be able to get around our preventive measures," added the president. "That's why these things are classified."

It's hard to believe, though, that the 560 million pages of classified documents the government produces each year all have to do with preventing terrorist acts or other matters related to national security. Often documents are classified because they would otherwise prove embarrassing to government officials — as in the WikiLeaks disclosure of Hillary Clinton's private opinion of certain foreign dignitaries. What's surprising is not that such things get leaked and published, but that they ever make their way into classified documents in the first place.

Perhaps our government officials are now embarrassed by what we've learned about the extent of their collection of data on us. In the statement they posted on their website, Google CEO Larry Page and chief legal officer David Drummond said they understand that governments "need to take action to protect their citizens' safety — including sometimes by using surveillance. But the level of secrecy around the current legal procedures undermines the freedoms we all cherish."

Photo of President Obama: AP Images