



# U.S. secretly collecting huge number of phone records

*Director of National Intelligence James Clapper says leaks could cause long-lasting harm*

June 6, 2013

---

A leaked document has laid bare the monumental scope of the government's surveillance of Americans' phone records — hundreds of millions of calls — in the first hard evidence of a massive data collection program aimed at combating terrorism under powers granted by Congress after the 9/11 attacks.

At issue is a court order, first disclosed Wednesday by The Guardian newspaper in Britain, that requires the communications company Verizon to turn over on an "ongoing, daily basis" the records of all landline and mobile telephone calls of its customers, both within the U.S. and between the U.S. and other countries. Intelligence experts said the government, though not listening in on calls, would be looking for patterns that could lead to terrorists — and that there was every reason to believe similar orders were in place for other phone companies.

Some critics in Congress, as well as civil liberties advocates, declared that the sweeping nature of the National Security Agency program represented an unwarranted intrusion into Americans' private lives. But a number of lawmakers, including some Republicans who normally jump at the chance to criticize the Obama administration, lauded the program's effectiveness. Leaders of the House Intelligence Committee said the program had helped thwart at least one attempted terrorist attack in the United States, "possibly saving American lives."

Separately, The Washington Post and The Guardian reported Thursday the existence of another program used by the NSA and FBI that scours the nation's main Internet companies, extracting audio, video, photographs, emails, documents and connection logs to help analysts track a person's movements and contacts. It was not clear whether the program, called PRISM, targets known suspects or broadly collects data from other Americans.

The companies include Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. The Post said PalTalk has had numerous posts about the Arab Spring and the Syrian civil war. It also said Dropbox would soon be included.

Google, Facebook, Yahoo, Microsoft and Apple said in statements that they do not provide the government with direct access to their records.

"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," the company said.

### **National intelligence director says leaks could cause harm**

The leaks about the programs brought a sharp response from James Clapper, the director of national intelligence. In an unusual statement late Thursday, Clapper called disclosure of the internet surveillance program "reprehensible" and said the leak about the phone record collecting could cause long-lasting and irreversible harm to the nation's ability to respond to threats.

**'If you're not getting a call from a terrorist organization, you've got nothing to worry about.'**—*Republican Sen. Lindsey Graham*

Clapper said news reports about the programs contained inaccuracies and omitted key information. He declassified some details about the authority used in the phone records program because he said Americans must know the program's limits. Those details included that a special national security court reviews the program every 90 days and that the court prohibits the government from indiscriminately sifting through phone data. Queries are only allowed when facts support reasonable suspicion, Clapper said.

Sen. Ron Wyden, a Democrat from Oregon, said of the phone-records collecting: "When law-abiding Americans make phone calls, who they call, when they call and where they call is private information. As a result of the discussion that came to light today, now we're going to have a real debate."

But Republican Sen. Lindsey Graham of South Carolina said Americans have no cause for concern. "If you're not getting a call from a terrorist organization, you've got nothing to worry about," he said.

A senior administration official pointed out that the collection of communication cited in the Washington Post and Guardian articles involves "extensive procedures, specifically approved by the court, to ensure that only non-U.S. persons outside the U.S. are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about U.S. persons." The official, who was not authorized to discuss the matter publicly and requested anonymity, added that Congress had recently reauthorized the program.

Senate Intelligence Committee Chairwoman Dianne Feinstein, a Democrat from California, said the order was a three-month renewal of an ongoing practice that is supervised by federal judges who balance efforts to protect the country from terror attacks against the need to safeguard Americans' privacy. The surveillance powers are granted under the post-9/11 Patriot Act, which was renewed in 2006 and again in 2011.

While the scale of the program might not have been news to some congressional leaders, the disclosure offered a public glimpse into a program whose breadth is not widely understood. Sen.

Mark Udall, a Colorado Democrat who serves on the Intelligence Committee, said it was the type of surveillance that "I have long said would shock the public if they knew about it."

The government has hardly been forthcoming.

Wyden released a video of himself pressing Director of National Intelligence James Clapper on the matter during a Senate hearing in March.

"Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Wyden asked.

"No, sir," Clapper answered.

"It does not?" Wyden pressed.

Clapper quickly softened his answer. "Not wittingly," he said. "There are cases where they could, inadvertently perhaps, collect — but not wittingly."

There was no immediate comment from Clapper's office Thursday on his testimony in March.

The public is now on notice that the government has been collecting data — even if not listening to the conversations — on every phone call every American makes, a program that has operated in the shadows for years, under President George W. Bush, and continued by President Barack Obama.

"It is very likely that business records orders like this exist for every major American telecommunication company, meaning that if you make calls in the United States the NSA has those records," wrote Cindy Cohn, general counsel of the nonprofit digital rights group Electronic Frontier Foundation, and staff attorney Mark Rumold, in a blog post.

Without confirming the authenticity of the court order, White House spokesman Josh Earnest said such surveillance powers are "a critical tool in protecting the nation from terror threats," by helping officials determine if people in the U.S. who may have been engaged in terrorist activities have been in touch with other known or suspected terrorists.

House Intelligence Committee Chairman Mike Rogers, a Republican from Michigan, stressed that phone records are collected under court orders that are approved by the Senate and House Intelligence committees and regularly reviewed.

### **'This isn't anything that's brand new'**

And Senate Democratic leader Harry Reid of Nevada played down the significance of the revelation.

"Everyone should just calm down and understand that this isn't anything that's brand new," he said. "This is a program that's been in effect for seven years, as I recall. It's a program that has worked to prevent not all terrorism but certainly the vast, vast majority. Now is the program perfect? Of course not."

But privacy advocates said the scope of the program was indefensible.

"This confirms our worst fears," said Alexander Abdo, a staff attorney with the American Civil Liberties Union's National Security Project. "If the government can track who we call," he said, "the right to privacy has not just been compromised — it has been defeated."

Rep. Jim Sensenbrenner, a Republican from Wisconsin, who sponsored the USA Patriot Act that governs the collection, said he was "extremely troubled by the FBI's interpretation of this legislation."

Attorney General Eric Holder sidestepped questions about the issue during an appearance before a Senate subcommittee, offering instead to discuss it at a classified session that several senators said they would arrange.

House Speaker John Boehner called on Obama to explain why the program is necessary.

It would "be helpful if they'd come forward with the details here," he said.

The disclosure comes at a particularly inopportune time for the Obama administration. The president already faces questions over the Internal Revenue Service's improper targeting of conservative groups, the seizure of journalists' phone records in an investigation into who leaked information to the media, and the administration's handling of the terrorist attack in Libya that left four Americans dead.

At a minimum, it's all a distraction as the president tries to tackle big issues like immigration reform and taxes. And it could serve to erode trust in Obama as he tries to advance his second-term agenda and cement his presidential legacy.

The Verizon order, granted by the secret Foreign Intelligence Surveillance Court on April 25 and good until July 19, requires information on the phone numbers of both parties on a call, as well as call time and duration, and unique identifiers, according to The Guardian.

**"The law authorizes the federal courts to order a company to provide information in certain circumstances, and if Verizon were to receive such an order, we would be required to comply."**—*Verizon executive vice president and general counsel Randy Milch*

It does not authorize snooping into the content of phone calls. But with millions of phone records in hand, the NSA's computers can analyze them for patterns, spot unusual behavior and identify "communities of interest" — networks of people in contact with targets or suspicious phone numbers overseas.

Once the government has zeroed in on numbers that 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.

Rogers said once the data has been collected, officials still must follow "a court-approved method and a series of checks and balances to even make the query on a particular number."

But Jim Harper, a communications and privacy expert at the libertarian-leaning Cato Institute, questioned the effectiveness of pattern analyses to intercept terrorism. He said that kind of analysis would produce many false positives and give the government access to intricate data about people's calling habits.

Verizon executive vice-president and general counsel Randy Milch, in a blog post, said the company isn't allowed to comment on any such court order.

"Verizon continually takes steps to safeguard its customers' privacy," he wrote. "Nevertheless, the law authorizes the federal courts to order a company to provide information in certain circumstances, and if Verizon were to receive such an order, we would be required to comply."

The company listed 121 million customers in its first-quarter earnings report this April — 98.9 million wireless customers, 11.7 million residential phone lines and about 10 million commercial lines.

The NSA had no immediate comment. The agency is sensitive to perceptions that it might be spying on Americans. It distributes a brochure that pledges the agency "is unwavering in its respect for U.S. laws and Americans' civil liberties — and its commitment to accountability."

Under Bush, the NSA built a highly classified wiretapping program to monitor emails and phone calls worldwide. The full details of that program remain unknown, but one aspect was to monitor massive numbers of incoming and outgoing U.S. calls to look for suspicious patterns, said an official familiar with the program. That official spoke on condition of anonymity because he was not authorized to discuss it publicly.

After The New York Times revealed the existence of that wiretapping program, the data collection continued under the Patriot Act, the official said. The official did not know if the program was continuous or whether it stopped and restarted at times.

The FISA court order, signed by Judge Roger Vinson, compelled Verizon to provide the NSA with electronic copies of "all call detail records or telephony metadata created by Verizon for communications between the United States and abroad" or "wholly within the United States, including local telephone calls," The Guardian said.

The law on which the order explicitly relies is the "business records" provision of the Patriot Act.