NSA chief drops hint about ISP Web, email surveillance

A secret interpretation of the Patriot Act led to the National Security Agency vacuuming up all of Verizon's phone logs. The NSA may be doing the same for e-mail and Web-browsing logs too.

By: Declan McCullagh – June 13, 2013

The head of the National Security Agency hinted Wednesday that logs of Americans' e-mails and Web-site visits may be secretly vacuumed up by the world's most powerful intelligence group. During a U.S. Senate hearing, NSA director Keith Alexander was asked specifically about whether "e-mail contacts" are ingested under the Obama administration's secret interpretation of the Patriot Act's surveillance powers.

"I don't want to make a mistake" and reveal too much, Alexander said, adding that disclosing details about such surveillance would cause "our country to lose some sort of protection." It would be appropriate, he said, to discuss e-mail and other metadata surveillance in a "classified session" that senators are scheduled to attend Thursday.

Among the small circle of outsiders who closely follow the NSA, the agency's close, long-standing relationship with AT&T, Verizon, and other telecommunications providers is an open secret -- so it would come as little surprise to find they're serving up exabytes of daily e-mail and Web-browsing logs as well. The Wall Street Journal reported last week, citing former government officials, that the NSA "obtains access to data from Internet service providers on Internet use such as data about e-mail or Web site visits."

But Wednesday's exchange between NSA director Alexander and Sen. Mike Johanns, a Nebraska Republican, appears to be the closest the Fort Meade, Md.-based agency has come to addressing the topic in a public setting.

"It would be odd [for the NSA] to focus entirely on telephony logs and exclude Internet traffic," said Julian Sanchez, a research fellow at the Cato Institute in Washington, D.C., who focuses on electronic surveillance topics. "I would assume they're vacuuming up IP logs and perhaps e-mail headers as well."

What prompted Wednesday's Senate exchange was a disclosure last week by the U.K.-based Guardian newspaper of a top-secret order from the U.S. Foreign Intelligence Surveillance Court. It allows the NSA to obtain daily records of all domestic calls made by Verizon customers. Subsequent reports said AT&T and Sprint are also involved.

The Justice Department obtained that order by claiming it was permitted by Section 215 of the Patriot Act, 50 USC 1861, better known as the "business records" portion. Section 215 allows FBI

agents to obtain any "tangible thing," including "books, records, papers, documents, and other items," which some of the Patriot Act's supporters have said was never intended to cover every American's phone call logs. (Section 215 orders are far less privacy-protective, and therefore more legally problematic, than traditional search warrants backed by probable cause and signed by a judge.)

In an unusual move, however, the Justice Department has refused to disclose its secret interpretation of Section 215 -- despite complaints from multiple senators -- that would reveal just how far Patriot Act surveillance has extended.

"What I worry is how far you believe this authority extends," Sen. Johanns said to the NSA director during Wednesday's hearing. Alexander replied that Section 215 only covered metadata: "If you want to get the content, you'd have to get a court order."

Under the Justice Department's reasoning, Web-browsing logs and e-mail logs "would seem to be a record, and thus potentially subject to a 215 order," said Kurt Opsahl, a senior staff attorney at the Electronic Frontier Foundation.

Any company running an e-mail server is likely to keep logs of incoming and outgoing messages, which would include metadata but not the content of the communication. While it's less clear which Internet service providers keep logs of customers' visits to Web sites, a document the ACLU obtained in 2010 sheds some light on the topic.

The document, an internal Justice Department chart marked "law enforcement use only," reveals that Verizon Wireless keeps "IP destination information," meaning records of what Internet Protocol addresses are visited, for 90 days. Sprint keeps connection logs for 60 days. T-Mobile, AT&T, and Virgin Mobile do not retain connection logs at all.

Alan Butler, appellate advocacy counsel at the Electronic Privacy Information Center in Washington, D.C., said he believes the Justice Department's use of Section 215 to obtain billions of phone records is illegal. But, he said, the department could nevertheless argue that IP address records should be treated the same as phone numbers:

> I think that IP address records would likely be treated the same as call records unless they contain "content" (detailed URIs for specific pages might be considered content). So the FBI could theoretically put forth the same broad relevance argument used to justify this Verizon order.

There's no evidence that Silicon Valley companies, which last week were incorrectly accused of opening their systems to the NSA, would acquiesce to a legally questionable use of Section 215, especially after their willingness to litigate over the legality of "national security letter" requests. In addition, Facebook CEO Mark Zuckerberg and Google CEO Larry Page have offered categorical denials of turning over such a collection of data to the federal government.

James Bamford, in his 2008 book "The Shadow Factory," described Internet service providers' participation in President Bush's now-reshaped warrantless wiretapping program as:

> For decades, AT&T and much of the rest of the telecommunications industry have had a very secret, very cozy relationship with the NSA... [NSA Director Michael Hayden] succeeded in gaining the secret cooperation of nearly all of the nation's telecommunications giants for his warrantless eavesdropping program. Within a year, engineers were busy installing highly secret,

heavily locked rooms in key AT&T switches, among them Bridgeton, New York City, and the company's major West Coast central office in San Francisco. From then on the data -- including both address information and content -- would flow through the PacketScopes directly to the NSA.

Other reports have suggested that the NSA uses metadata, which would include phone numbers, IP addresses, and e-mail addresses, to determine which person's communications to intercept. Once that task is complete, and legal process is satisfied, the taps at AT&T and other Internet providers would be used to target that person for heightened surveillance.

Heightening speculation about undisclosed NSA surveillance activities was what Rep. Loretta Sanchez (D-Calif.) said after attending a classified briefing Wednesday.
"What we learned in there," Sanchez said, "is significantly more than what is out in the media today."