

Denials in surveillance program require decoding

MICHAEL LIEDTKE - AP Technology Writer - Associated Press

Google CEO Larry Page and Facebook chief executive Mark Zuckerberg are denying reports that depict two of the Internet's most influential companies as willing participants in a secret government program that gives the National Security Agency unfettered access to email and other personal information transmitted on various online services.

The rebuttals issued Friday in blog posts expand upon earlier statements that the companies issued in an attempt to distance themselves from a government surveillance program that is raising questions. At issue is whether the NSA has constructed a direct pipeline into the computers that run some of the world's most widely used online services.

Each of the statements issued by Google Inc., Facebook Inc. and the five other companies linked to the program has been carefully worded in ways that doesn't rule out the possibility that the NSA has been gathering online communications as part of its efforts to uncover terrorist plots and other threats to U.S. national security.

"I think a lot of people are spending a lot of time right now trying to parse those denials," says Lee Tien, a senior staff attorney at the Electronic Frontier Foundation, a digital rights group. "The top level point is simply: it's pretty hard to know what those denials mean."

Google and Facebook were tied to a clandestine snooping program code-named PRISM in reports published late Thursday by The Washington Post and The Guardian, a British newspaper. James Clapper, the director of national intelligence for the Obama administration, subsequently confirmed PRISM had been approved by a judge and is being conducted in accordance with U.S. law.

But Clapper didn't identify what companies fall under PRISM's broad authority, leaving the reports by the Post and Guardian as the only windows into the spying program. The newspapers based their reports on confidential slides and other documents about PRISM.

Besides Google and Facebook, those documents cited Microsoft Corp., Apple Inc., Yahoo Inc., AOL Inc. and Paltalk as the other companies immersed in PRISM. The NSA program also is getting data from Google's YouTube video service and Microsoft's Skype chat service, according to the PRISM documents posted on the Post's website.

All of the companies have issued statements making it clear that they aren't voluntarily handing over user data. They also are emphatically rejecting newspaper reports indicating that PRISM has opened a door for the NSA to tap directly on the

Denials in surveillance program require decoding

Published on Electronic Component News (<http://www.ecnmag.com>)

companies' data centers whenever the government pleases.

"Press reports that suggest that Google is providing open-ended access to our users' data are false, period," Page asserts in a blog post co-written with Google's top lawyer, David Drummond.

In his post, Zuckerberg lambasts the media accounts as "outrageous."

All the companies but Microsoft and Yahoo said they had never heard of PRISM before the name was revealed Thursday.

All of the statements could be technically true. At the same time, they could mean the companies have been turning over user data when served a legally binding order issued under a program that they didn't know had a code name until they read about it like the rest of the world.

It's all part of a linguistic tango that's often performed when the cover is blown on a top-secret operation, Tien says. "The person could say 'That story is not true' and then say 'We have never done X,' pointing to the 5 percent that was in fact, inaccurate," he says. "A company could say "'We've never heard of the PRISM program.' Well, maybe the government didn't call it that. Or the company could say "'We don't allow backdoor access!' Well, maybe they allow front door access."

The companies tied to PRISM also are limited by law in how much they can say. They are prohibited from disclosing their compliance with orders issued under the Foreign Intelligence Surveillance Act of 1978. That law hatched the Foreign Intelligence Surveillance Court, whose activity is considered to be classified.

Microsoft began turning over data in 2007 on the sixth anniversary of the 9/11 terrorist attacks, according to the PRISM slides obtained by the Post. The documents list the following start dates for data collection at the other companies and services: Yahoo, March 2008; Google, January 2009; Facebook, June 2009; Paltalk, December 2009; YouTube, September 2010; Skype, February 2011; AOL, March 2011; Apple, October 2012.

In their posts, both Page and Zuckerberg seem to be telegraphing to the world that Google and Facebook are doing their best to limit the amount of user data that's being handed over to the U.S. government.

To do so, they both cite disclosures earlier this week that Verizon Communications has been providing the NSA with portions of the calling records for all its U.S. customers since late April. The disclosures being made under court order cover an estimated 3 billion calls per day.

"We were very surprised to learn that such broad orders exist," Page writes in his post. "Any suggestion that Google is disclosing information about our users' Internet activity on such a scale is completely false."

Zuckerberg also points out that Facebook has never received a government order

Denials in surveillance program require decoding

Published on Electronic Component News (<http://www.ecnmag.com>)

covering as much user data as the one that Verizon received. "If we did, we would fight it aggressively," he says in the post.

Both Page and Zuckerberg conclude their posts by imploring the government to be more forthcoming about the steps that it is taking to protect the public's safety.

"The level of secrecy around the current legal procedures undermines the freedoms we all cherish," Page writes.

—
AP Technology Writer Peter Svensson in New York contributed to this story.

Source URL (retrieved on 04/16/2014 - 9:40pm):

<http://www.ecnmag.com/news/2013/06/denials-surveillance-program-require-decoding>