THE DAILY BEAST
READ THIS SKIP THAT

Internet Companies Deny They're Helping the NSA Collect User Data. Should We Believe Them?

By: Megan McArdle – June 7, 2013

Just in case you weren't anxious enough about your cell phone, yesterday, theGuardian and the Washington Post dropped news that the NSA is also collecting data from multiple internet providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple. Dropbox is allegedly coming soon.

Yet the companies appear to be offering flat denials:

> An Apple spokesman said: "We have never heard of PRISM. We do not provide any government agency with direct access to our servers and any agency requesting customer data must get a court order," he said.
>
> Joe Sullivan, Facebook's chief security officer, said it did not provide government organisation with direct access to Facebook servers. "When Facebook is asked for data or information about specific individuals, we carefully scrutinise any such request for compliance with all applicable laws, and provide information only to the extent required by law."
>
> A Google spokesman also said it did not provide officials with access to its servers. "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'backdoor' into our systems, but Google does not have a 'back door' for the government to access private user data."
>
> Microsoft said it only turned over data when served with a court order: "We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don't participate in it."

> A Yahoo spokesman said: "Yahoo! takes users' privacy very seriously. We do not provide the government with direct access to our servers, systems, or network.

What to make of this? It would be stupid for them to deny this, and then get sued by their customers when it turns out it's not true.

Last night on Twitter, my husband outlined five possibilities:

1. The companies are lying

2. Only a few people in the company know about this, and they aren't issuing the statements

3. The Post and the Guardian are wrong and have been duped

4. PRISM was operating without the knowledge of the companies

5. The companies know, and those statements are very carefully worded.

All of these are in some way unbelievable. #1 is asking for a class action suit that destroys your company. #3 involves some very suspicious national security reporters at two different outlets simultaneously getting duped. And #2 strikes me as extremely unlikely. I can imagine one rogue employee doing this without telling his employers. I cannot imagine the exact same thing happening at nine of the biggest internet companies.

The most likely possibilities seem to be #4 or #5: the NSA is filtering this stuff at some point outside the companies, or the companies have issued some very, very carefully worded statements.

It's impossible to say for sure which it is. But as Julian Sanchez, the Cato Institute's tech privacy expert, points out, there may be a clue in the statements. "All the denials can be literally technically true without anything in the story being substantively false," he told me. "We've never heard of PRISM" might just mean "They didn't tell us the codename!" Likewise, Facebook and Microsoft's statements add up to saying they don't do this sort of thing voluntarily.

The Washington Post suggests that ambiguous in the original NSA slides may have given them a window to issue non-denial denials: "It is possible that the conflict between the PRISM slides and the company spokesmen is the result of imprecision on the part of the NSA author. In another classified report obtained by The Post, the arrangement is described as allowing 'collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations,' rather than directly to company servers."

"Most likely, to my mind," says Sanchez, "is that they've got something akin to the "Secret Room" that Mark Klein disclosed in AT&T hubs where traffic is being cloned (the companies would need to provide the relevant SSL encryption keys) split off into NSA's own machines. It would be literally true, in that case, that the NSA does not have direct access to *Google's* servers." But they would still have access to a lot of data.

"Alternatively, they could just be plucking the encryption keys for the sessions they want from the partner companies and then copying the actual traffic via their facilities at the Internet Service Provider level."

The Post also argues that the NSA would need inside help, even if they're technically collecting the data elsewhere.

If it does turn out that they've been issuing statements that were technically true, but utterly misleading, that may save them from lawsuits. But it will not save them from the customer backlash. Indeed, that could be worse, if people decide to trust them, and then later realize they were duped. In general, crisis managers tend torecommend against absolute denial in cases where the truth might come out; once the public thinks that you lied (rather than just not telling them something), they tend to be unforgiving.

On the other hand, as I noted yesterday, the American public has been amazingly quiescent in the face of previous revelations about extensive surveillance. Perhaps the companies are relying on them to once again roll their eyes and then log right back in.

Like The Daily Beast on Facebook and follow us on Twitter for updates all day long.

Megan McArdle is a special correspondent for *Newsweek* and The Daily Beast covering business, economics, and public policy. A former senior editor at *The Atlantic* and writer for *The Economist*, Megan has a diverse work history including three small startups and a disaster recovery firm at Ground Zero.