the Atlantic

Why Did *60 Minutes* Let the Head of the NSA Fool Its Audience?

CBS presented General Alexander's highly misleading answer in a way that guaranteed most viewers would be misled.

By: Conor Friedersdorf - December 16 2013,

Consider the following exchange from Sunday's *60 Minutes* interview between the head of the NSA, General Keith Alexander, and CBS News correspondent John Miller. The subject is the NSA gathering of bulk Internet data while overseas.

This week, the CEOs of eight major Internet providers including Google, Apple and Yahoo asked the president for new limits to be placed on the NSA's ability to collect personal information from their users.

John Miller: One of the Snowden leaks involved the concept that NSA had tunneled into the foreign data centers of major U.S. Internet providers. Did the leak describe it the right way?

Gen. Keith Alexander: No, that's not correct.

We do target terrorist communications. And terrorists use communications from Google, from Yahoo, and from other service providers. So our objective is to collect those communications no matter where they are. But we're not going into a facility or targeting Google as an entity or Yahoo as an entity. But we will collect those communications of terrorists that flow on that network.

How could *60 Minutes* broadcast that exchange as is?

* * *

In order to understand what happened here and why it's misleading to viewers, it's useful to look back at the *Washington Post* story to which the question apparently refers:

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

The article goes on to explain how this overseas data-gathering works and why it is done:

According to a top-secret accounting dated Jan. 9, 2013, **the NSA's acquisitions directorate sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency's headquarters at Fort Meade, Md.** In the preceding 30 days, the report said, field collectors had

processed and sent back 181,280,466 new records—including “metadata,” which would indicate who sent or received e-mails and when, as well as content such as text, audio and video.

... Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight. NSA documents about the effort refer directly to “full take,” “bulk access” and “high volume” operations on Yahoo and Google networks. Such large-scale collection of Internet content would be illegal in the United States, but the operations take place overseas, where the NSA is allowed to presume that anyone using a foreign data link is a foreigner.

A subsequent *New York Times* story is also relevant, as you'll soon see. That story reported on how the NSA bypassed company data centers and tapped fiber-optic cables that connect them:

SAN FRANCISCO — The recent revelation that the National Security Agency was able to eavesdrop on the communications of Google and Yahoo users **without breaking into either company’s data centers** sounded like something pulled from a Robert Ludlum spy thriller. How on earth, the companies asked, did the N.S.A. get their data without their knowing about it? The most likely answer is a modern spin on a century-old eavesdropping tradition.

People knowledgeable about Google and Yahoo’s infrastructure say they believe that **government spies bypassed the big Internet companies and hit them at a weak spot — the fiber-optic cables that connect data centers** around the world and are owned by companies like Verizon Communications, the BT Group, the Vodafone Group and Level 3 Communications. In particular, fingers have been pointed at Level 3, the world’s largest so-called Internet backbone provider, whose cables are used by Google and Yahoo.

In his question, Miller should have said is something like, "One of the Snowden leaks reported that the NSA intercepted data flowing between the foreign data centers of major Internet firms. Is that right?" The truthful answer would be, "Yes, that's right."

Instead, Miller said, "One of the Snowden leaks involved the concept that NSA had **tunneled into the foreign data centers** of major U.S. Internet providers. **Did the leak describe it the right way**?" That's a terrible way to phrase the question if you're dealing with an NSA employee intent on exploiting any loophole.

And Alexander's answer still wasn't totally responsive.

"No, that's not correct," he began. What's not correct? The NSA documents that Snowden leaked? The *Washington Post* story? Miller's summary of it? It's left unclear.

Alexander continued: "We do target terrorist communications. And terrorists use communications from Google, from Yahoo, and from other service providers. So our objective is to collect those communications no matter where they are. But we're not going into a facility or targeting Google as an entity or Yahoo as an entity. But we will collect those communications of terrorists that flow on that network."

This is a classic technically-accurate-but-wildly-misleading NSA answer. As best as I can understand the thought process behind Alexander's evasions, it's something like this: No, the NSA isn't "tunneling" or "going into a facility." It is copying data flows as they pass *between* facilities. No, the NSA isn't "targeting Google" or Yahoo "as an entity." Its "targets"—per the highly particular NSA meaning of that word—are users who communicate via Google and Yahoo. Of course, by intercepting data as it flows between foreign Google and Yahoo facilities, the NSA is getting the same stuff as it would get if it were "targeting" Google and Yahoo by "tunneling" into their foreign facilities.

(Alexander may also be relying on the fact that GCHQ, the NSA's British counterpart, is technically the entity doing some of the work.)

Ultimately, only Alexander himself knows exactly what technicalities he used to obscure the truth here. What's clear is that because of the imprecise way Miller asked his question, the misleading way Alexander answered it, Miller's failure to ask follow-up questions to clarify the truth, and *60 Minutes*' decision to air the exchange without further explanation, the news program all but guaranteed that the vast majority of its audience would come away with an inaccurate impression on this matter. Alexander makes it sound as if, in the course of tracking individual terrorists, the NSA happens to collect some data from Google and Yahoo, because sometimes terrorists use those platforms.

But as the *Washington Post* explained, the NSA had a particular slide about "Google Cloud Exploitation":

Google and Yahoo ... had reason to think, insiders said, that their private, internal networks were safe from prying eyes. In an NSA presentation slide on “Google Cloud Exploitation,” however, a sketch shows where the “Public Internet” meets the internal “Google Cloud” where their data reside. In hand-printed letters, the drawing notes that encryption is “added and removed here!” The artist adds a smiley face, a cheeky celebration of victory over Google security.

Two engineers with close ties to Google exploded in profanity when they saw the drawing. “I hope you publish this,” one of them said. For the MUSCULAR project, the GCHQ directs all intake into a “buffer” that can hold three to five days of traffic before recycling storage space. From the buffer, custom-built NSA tools unpack and decode the special data formats that the two companies use inside their clouds. Then the data are sent through a series of filters to “select” information the NSA wants and “defeat” what it does not.

PowerPoint slides about the Google cloud, for example, show that the NSA tries to filter out all data from the company’s “Web crawler,” which indexes Internet pages.

According to the briefing documents, prepared by participants in the MUSCULAR project, collection from inside Yahoo and Google has produced important intelligence leads against hostile foreign governments that are specified in the documents.

Notice how Alexander managed to make it sound like the *Washington Post* got something wrong without contradicting anything actually reported in the *Post* story—even as he made what the NSA does sound a lot less intrusive than it actually is.

As ever, an unfamiliar definition of "target" does much of his work.

Julian Sanchez of The Cato Institute puts things in perspective. "Since the initial debate about the FISA Amendments Act," he says, "intelligence officials have focused insistently on 'targeting' rather than 'collection,' as though civil liberties concerns about the acquisition of Americans' communications on a vast scale are frivolous, provided only foreigners—and it's certainly not just foreign 'terrorists,' by the way—are the 'targets.' This is, when you think about it, quite perverse. The general warrants so despised by the framers of our Constitution didn't 'target' a particular individual either—but that didn't somehow make them acceptable; it was the heart of the problem! It amounts to an argument that you should't object to the government seizing your private correspondence on the grounds that you aren't the one under suspicion. It has apparently become quaint to object that this is precisely why one's correspondence shouldn't be seized."