

# ILLEGAL SPYING ON HACKERS

I'm going to have plenty to say on Shane Harris' story revealing that the NSA used hackers and foreign cyberhacks as their excuse for illegally accessing customer data prior to 9/11. First, though, I'd like to remind readers of this earlier Shane Harris story (with Tim Naftali)—to my mind the best reporting on this topic outside of the Risen-Lichtblau early scoop.

A former telecom executive told us that efforts to obtain call details go back to early 2001, predating the 9/11 attacks and the president's now celebrated secret executive order. The source, who asked not to be identified so as not to out his former company, reports that the NSA approached U.S. carriers and asked for their cooperation in a "data-mining" operation, which might eventually cull "millions" of individual calls and e-mails.

In other words, nearly two years ago, Harris (with Naftali) quoted a telecom executive saying that something had gone on earlier than 9/11. And now, he's providing details about Qwest's refusal to cooperate.

## The Rationale

So, returning to this story after Nacchio's appeal has raised a lot of questions about the earlier request, Harris reveals the rationale the Administration offered for its earlier data mining.

However, in February 2001, the NSA's primary purpose in seeking access to Qwest's network apparently was not to search for terrorists but to watch for computer hackers and foreign-government forces trying to penetrate and compromise U.S. government information

systems, particularly within the Defense Department, sources said.

Government officials have long feared a "digital Pearl Harbor" if intruders were to seize control of these systems or other key U.S. infrastructure through the Internet.

[snip]

[former NSA Director] Minihan singled out Russia and China; the latter, he said, had already incorporated cyber-warfare into its military training. He also pointed to the emergence of "transnational security challenges," including terrorism, drug trafficking, and international organized crime. "These opportunists, enabled by the explosion of technology and the availability of inexpensive, secure means of communication, pose a significant threat to the interests of the United States and its allies," Minihan said.

Harris also gives a general sense of how the program was justified as legal.

A former senior NSA official said that the agency also worried that because these groups understood privacy laws so well, they knew how to avoid detection and could predict what the NSA would, and wouldn't, do to track them. "There was such a nuanced understanding of how to tie us in knots and use American law against us, that there were certainly pockets of people saying, 'We've got to be assertive; we've got to be more aggressive on this,' " the former official said.

Hayden, who ran the NSA from 1999 to 2005, was well known for his willingness to push operations to the legal edge. "We're pretty aggressive within the law,"

Hayden said in public remarks after 9/11. "As a professional, I'm troubled if I'm not using the full authority allowed by law."

Hayden has repeated that refrain since the attacks. But former intelligence officials doubted that he would have authorized any request to Qwest, or other companies, that he believed violated the law. **They noted, however, that many in the agency had long thought that monitoring "metadata," such as a phone number, the length of a call, or a series of calls placed from a particular phone, didn't implicate privacy because such information didn't constitute the "content" of a message – its written or spoken words.** [my emphasis]

This excuse sounds **precisely** like public denials about the program Hayden made after the NYT revealed the problem with the program involved data mining (this quote is a riff on a Glenn Greenwald quote).

In January, 2006, Gen. Michael Hayden – the NSA Director during the implementation of the "TSP" and the current CIA Director – gave a press briefing at the National Press Club in which he **emphatically denied that the NSA had been engaging in *the type of "data mining" which this morning's articles describe.*** During his opening remarks, Hayden said:

Let me talk for a few minutes also about what this program is not. It is not a drift net over Dearborn or Lackawanna or Fremont ***grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts kept talking about.***

This is targeted and focused. This is not about intercepting conversations between people in the United States. This is hot pursuit of communications entering or leaving America involving someone we believe is associated with al Qaeda.

Hethen made clear that the NSA could not and would not engage in such data mining because of the "ethical" and "practical" considerations involved: QUESTION: Are you spying on or intercepting our communications, e-mails and telephone conversations of those of us who are organizing The World Can't Wait to Drive Out the Bush Regime?

GEN. HAYDEN: You know, I tried to make this as clear as I could in prepared remarks. I said this isn't a drift net, all right? I said **we're not there sucking up coms and then using some of these magically alleged keyword searches** – "Did he say 'jihad'?"

[bold Glenn's; italics mine]

In other words, faced with the anonymous description that the problem with the warrantless wiretap program had to do with data mining, Hayden neatly parsed that it couldn't be data mining because they didn't "[suck] up coms and then [use] some of those magically alleged keyword searches." Hayden denied that they had mined content, but he stopped well short of saying that they hadn't mined metadata.

Which strongly suggests that Michael Hayden was well aware that the NSA was mining metadata, long before 9/11.