THE DAILY BEAST

Former NSA Director Michael Hayden Responds To Edward Snowden Claim

After a week of explosive disclosures, former NSA officials come out to say what the highly secretive agency does, and does not, do.

By: Eli Lake – June 12, 2013

One of the most startling disclosures from Edward Snowden, the former National Security Agency contractor who leaked top secret documents to *The Guardian* and*The Washington Post* was that he could tap into the private email of any American citizen—even President Obama—from his desk station in Hawaii.

Former top NSA officials interviewed by The Daily Beast Tuesday, however, say Snowden's claim that systems administrators like himself could eavesdrop on U.S. citizens is incorrect, and that any NSA employee that targeted even a foreign source for personal reasons would be stripped of clearances and fired on the spot.

"Not all analysts have the power to target anything," Snowden told *The Guardian* in an interview posted Sunday. "But I, sitting at my desk, had the authority to wiretap anyone, from you or your accountant to a federal judge to even the president if I had a personal email."
Michael Hayden, a former NSA director and CIA director, said Snowden's assertion was "absolutely outrageous." "He was not a collector," he said. "I don't know he could do anything like that," adding that Snowden, a low-ranking contractor, would not have the authority or access to listen in on phone calls or read emails from anyone.

It is difficult to evaluate the claims of the officials—or those of Snowden—because the organization operates in almost total secrecy. A running joke inside the intelligence community is that NSA stands for "no such agency."

Adding to the confusion is that even members of Congress, such as Senator Jon Tester, a Democrat from Montana, are now saying they were not fully informed about the dragnet collection of call records of U.S. telecom companies, and other data from internet companies. On Tuesday, lawyers from the Justice Department and the NSA briefed members of the House Permanent Select Committee on Intelligence on the two NSA programs disclosed by *The Guardian* and *The Washington Post*.
"Rogue collection" at the NSA over the years was extremely rare, the former top official said. Asked for an example, Hayden said he remembered a collector who was fired for trying to snoop on his ex-wife overseas.

“A rogue collector would lose his clearance and be run out of the organization,” said Joel Brenner, a former inspector general and senior counsel for the NSA who left the agency in 2010. Brenner said that he didn’t recall ever dealing with "rogue collecting" during his time at as inspector general.

What did occupy his time, said Brenner, was what he called errors and “over-collection”— information with no foreign intelligence value or unintentionally collected information about a U.S. person. “You’ve got to understand that over-collection is to some degree inevitable,” he said. “When you are taking information off of a fiber optic cable with unimaginably large volumes passing at the speed of light, you are going to get some stuff that has to be filtered out later.”

Another issue, Brenner said, is “analytical error,” when a collector who believes he or she was targeting a foreign person turned out to instead be targeting an American citizen. In such an instance, the NSA is compelled to eliminate the data that was collected. “If someone is making lots of errors they will get a talking-to.”

While the NSA has been rocked by the week’s disclosures, the agency appears to have anticipated a backlash against its mining of Internet data and call records. In February, the agency’s general counsel Rajesh De gave a public, if little noticed at the time, speech at Georgetown University responding to what he said were three “false myths” about the NSA: that “NSA is a vacuum that indiscriminately sweeps up and stores global communications;” that “NSA is spying on Americans at home and abroad with questionable or no legal basis;” and that “NSA operates in the shadows free from external scrutiny or any true accountability.”

De went onto lay out what he said were major legal restrictions imposed by the Foreign Intelligence Surveillance Act on NSA collection activities that require the agency to avoid using its spying capabilities to reverse target U.S. citizens or intentionally targeting U.S. persons. In cases where there is over-collection, De said there were “minimization procedures” to discard data that is not pertinent to foreign intelligence collection.

Despite this new openness about internal controls in the aftermath of Snowden’s leaks, outside critics remain worried about the powerful and secretive agency. Julian Sanchez, a research fellow at the libertarian Cato Institute, said he was concerned that the data the NSA was supposed to destroy would still be stored somewhere. “We don’t know what destroying the data means,” he said. “There is a case, *U.S. vs. Sattar,* where the government produced thousands of hours of intercepted communications that were minimized but not destroyed. When the NSA says the data is minimized it does not necessarily mean that it’s destroyed. It may just not be logged, indexed, or put into a report, but the data is still in the possession of the U.S. government.”

In his speech at Georgetown, De did not discuss the government’s secret interpretation of section 215 of the Patriot Act, exposed last week by *The Guardian*’s story disclosing a secret court order for Verizon to hand over telephone metadata records of its customers. The public law only says the U.S. government may demand business records from U.S. companies, but does not specify that this would include the highly detailed calling records the court order compelled Verizon to produce.

An author of the original Patriot Act, Wisconsin Republican James Sensenbrenner, wrote

Attorney General Eric Holder last week saying the secret interpretation was not in keeping with the original intent of the legislation.

The government relies on this interpretation of the law to continue the broad intelligence gathering that began with the Terrorist Surveillance Program started under the first term of President George W. Bush. Originally, this NSA program, which tracked every phone call coming in or out of the United States was not subject to any kind of judicial oversight. In 2006, the Foreign Intelligence Surveillance Act was amended to make the collection of the telephone metadata legal. The legal mechanism to collect this data from the phone companies was section 215 of the Patriot Act.

Hayden said that even when the terrorist surveillance program was not subject to court oversight, NSA officers sifting through the data at the agency's Ft. Meade headquarters were constantly aware that they were not allowed to spy on Americans.

"At the height of the terrorist surveillance program," said Hayden, when you walked into the office where this was being done, you saw these people work with headphones [and] there was a big sign hanging from the ceiling that said: 'What Constitutes a U.S. Person?'" He called the sign a reminder that the snooping in that room could not extend to Americans unless they were involved in an active terrorist plot.

More information may come to light about the NSA's activities with the American Civil Liberties Union announcement Tuesday that it would be suing the NSA over what it deemed the "dragnet" collection of domestic phone records.