ars technica
the art of technology

Five things Snowden leaks revealed about NSA's original warrantless wiretaps

Looking through call records? It was actually the telcos' idea.

By Julian Sanchez – July 9th, 2013

As stories based on Edward Snowden's trove of leaked National Security Agency (NSA) documents continue to trickle out, most reporters have focused on what they can tell us about the spy agency's current or recent surveillance activities. Yet one of the most interesting documents from Snowden's cache, published in full by *The Guardian* back in June, sheds new light on the granddaddy of them all: President Bush's original warrantless wiretap program.

It was this program, itself one component of a broader initiative known as STELLAR WIND, that kicked off the modern debate over NSA surveillance powers when it was exposed in a bombshell 2005 *New York Times* story. An unclassified report on the "President's Surveillance Program," jointly authored by the Inspectors General of the major intelligence agencies, was released in 2009. But the newly leaked classified draft report by the NSA's Inspector General (IG) has painted a far more complete picture of STELLAR WIND's genesis and evolution. Here are five of the most interesting details either revealed or confirmed in that classified draft.

The program was broader than originally reported

Both president Bush and members of his administration repeatedly stressed that the warrantless wiretap program was narrowly limited to "persons reasonably believed to be members or agents of al Qaeda or affiliated terrorist organizations." Perhaps that was true by the time the *New York Times* revealed the program's existence. But the description of the NSA's IG suggests that, at least initially, the president authorized far broader surveillance, encompassing all communications between the United States and Afghanistan. As the draft report explains:

The Authorization specified that NSA could acquire the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States.

The surveillance authorization changed over time, as the report notes, and it eventually dropped the specific reference to Afghanistan. Though the report does reference an appendix further detailing the evolution of the president's authorization over time, that document hasn't yet been

published. That means it's unclear whether other countries or regions—such as, say, Iraq or Pakistan—were later subject to similar blanket surveillance authorization.

Cheney's office wanted domestic communications

According to the IG report, the first version of the warrantless wiretap authorization was drafted by David Addington—then general counsel to Vice President Dick Cheney, now a vice president at the conservative Heritage Foundation—without any input or advice from either the NSA or Justice Department lawyers. Addington subsequently pointed out to NSA director Michael Hayden that his wording "could have been interpreted to allow domestic content collection where both communicants were in the US or were US persons." That's presumably because, according to the summary quoted above, the legal wording included a mandate to wiretap communications when "one communicant was engaged in or preparing for acts of international terrorism"—without specifying that the "communicant" had to be overseas.

It was apparently Hayden who declined to take that additional step, on the grounds that the NSA was both technically and legally set up for *foreign* intelligence collection. Of course, since the NSA was intercepting e-mail as well as phone calls, and it's not always easy to tell in advance where the parties to an e-mail exchange are located, it seems inevitable that plenty of totally domestic communications got vacuumed into the NSA's databases anyway.

The phone companies suggested using call records

After the attacks of September 11, 2001—but before President Bush authorized the program that would become STELLAR WIND on October 4—two major telecommunications companies approached the NSA to volunteer their assistance. Though they're identified only as "COMPANY A" and "COMPANY B" in the reports, experts agree that they are almost certainly AT&T and Verizon. One of them, COMPANY B, had even done some of its own freelance intelligence work: it told the NSA that it had "noticed odd patterns in domestic calling records surrounding the events of 11 September and offered call records and analysis."

Then again, perhaps "volunteer" isn't quite the right word. The report tallies the costs of the program, which came to a bit more than $146 million over fiscal years 2002–2006. But only about $44 million of that went to the software and hardware infrastructure needed to sift through all that data. By far the biggest expense category—accounting for the other $102 million in outlays—was the "metadata and content" itself, an apparent reference to payments to the participating telecoms.

It was also the companies that eventually drove the shift to the current version of the call records program, using the Patriot Act's "business records" authority (Section 215). After the publication of the *Times* exposé, company lawyers appear to have gotten skittish and decided they were no longer comfortable acting on a permission slip from the president; they wanted a court order to keep coughing up the data. (And they eventually got it.)

The scale of the snooping

The original *Times* story that exposed the wiretap component of STELLAR WIND gave an approximate measure of how many people were under warrantless surveillance at any given time: up to 500 in the US and 5,000-7,000 foreigners. But since names were added and dropped from the target lists over time, it was hard to know the total number of people the NSA

had spied on. The *Times* did quote anonymous officials suggesting that the number of domestic targets "may have reached into the thousands since the program began," however.

The IG report finally gives us some hard numbers—though it only counts the phone lines and e-mail addresses targeted for collection, not individual human targets, which seems likely to be a somewhat smaller figure. The NSA intercepted communications to or from a total of 37,644 e-mail addresses and phone numbers over the life of the program. About eight percent of the total—3,018—were believed to belong to Americans. Of course, an American didn't need to be targeted to get sucked into the NSA's vacuum cleaner; any conversation between someone in the US and one of those 34,646 foreign e-mail accounts or phone lines would have been tapped as well.

For reasons not detailed in the report, spying on e-mail seems to have been far more popular for foreign than domestic targets. Only about 406 domestic e-mail accounts were flagged for interception, compared with 2,612 phone numbers. For foreigners, by contrast, e-mail accounts substantially outnumbered flagged phone numbers, 19,000 to 15,646.

Secrecy impeded effective oversight

Though ultimately more than 3,000 people—mostly within the NSA—were read into the program, the initial secrecy around it was so intense that, notoriously, even the NSA's own lawyers weren't allowed to see the legal reasoning justifying it until 2004—something NSA officials themselves found strange.

That secrecy meant that the NSA's own Inspector General—the agency's primary internal watchdog—wasn't cleared to know about the program until August 2002, nearly a year after it began. Even that appears to have been a reluctant concession; NSA Director Michael Hayden had to "make a case" to the White House for reading the IG in. As a result, it was not until February 2003 that the IG "learned of PSP incidents or violations that had not been reported to overseers as required, because none had the clearance to see the report." The precise nature of those "incidents or violations" remains unknown.