CATO AT LIBERTY

JULY 19, 2013

What the Ashcroft 'Hospital Showdown' Was About

By Julian Sanchez

SHARE

We've known for years that the STELLAR WIND surveillance program authorized by President George W. Bush led to a dramatic "Hospital Showdown" at the bedside of then–attorney general John Ashcroft. Now, documents leaked by Edward Snowden have finally given us a clearer idea of what it was really all about.

The infamous showdown took place in March 2004, while Ashcroft was recovering from illness in a hospital bed. Acting attorney general James Comey—now President Obama's nominee to head the FBI—was refusing to reauthorize one component of the secret surveillance program, having concluded that it was illegal. This prompted White House counsel Alberto Gonzales to rush to Ashcroft's hospital room in hopes of getting the ailing AG to countermand Comey, who was tipped off about Gonzales' plan and sped there as well.

In the confrontation that ensued, Ashcroft supported Comey—both formally (because Comey was legally the attorney general while Ashcroft was incapacitated) and on the legal substance. When Bush reauthorized the program anyway, despite the Justice Department's conclusion that it was unlawful, Comey threatened to resign—with Ashcroft, FBI director Robert Mueller, and other top officials reportedly ready to join him. Bush ultimately backed down, and the troublesome component was briefly suspended until it could be renewed under a different legal authority.

In 2008, we learned that the central bone of contention wasn't warrantless wiretapping, but rather some form of data mining. And more recently, via reporting in the *Washington Post* and a classified NSA report leaked by *The Guardian*, we learned that the controversy specifically involved Internet, not telephone, metadata. That last document in particular makes it fairly clear what the controversy must have been about—at least if you're steeped in surveillance law. For those who aren't, this is what probably happened:

STELLAR WIND had four components, each corresponding to types of information that President Bush had authorized the NSA to collect without a court order:

- telephone content (i.e., warrantless wiretapping)
- Internet content
- telephone metadata (i.e., the massive call records database)
- Internet metadata

The administration had originally carried out this surveillance on a radical theory of "inherent presidential authority" spelled out by then–Justice Department lawyer John Yoo, which held that during wartime, the president's surveillance powers could not be constrained by Congress, or even the Fourth Amendment. After he returned to academia in 2003, however, his successors grew uncomfortable with his leaps of legal logic and stopped relying on his questionable opinions on a broad range of counterterrorism issues. To justify Bush's surveillance programs, DOJ lawyers switched to the theory, spelled out at length in a January 2006 white paper, that Congress's Authorization for the Use of Military Force (AUMF) against Al Qaeda and their affiliates had created a tacit exception to the Foreign Intelligence Surveillance Act (FISA). Though FISA is supposed to be the "exclusive means" by which intelligence surveillance is conducted, DOJ attorneys argued that the AUMF authority to use "all necessary and appropriate force" against those who the president "determines planned, authorized, committed or aided" the September 11 attacks necessarily included the power to conduct surveillance, superseding FISA's judicial review requirements.

That was far less radical than Yoo's argument, though still a pretty problematic bit of legal reasoning: Congress, after all, explicitly expanded the government's surveillance powers in the USA Patriot Act soon after, which suggests they didn't think they'd already given the president carte blanche in the AUMF. Moreover, the administration appears not to have asked for changes that would have made STELLAR WIND lawful at least in part out of fear that Congress would refuse. Still, that wasn't what Comey objected to: He and his colleagues seem to have accepted this general line of reasoning when it came to warrantless

wiretapping.

The presidential authorization to intercept telephone and Internet *content*, however, was at least somewhat limited: Though no court oversight was required, NSA had to believe that the target of its taps was in Afghanistan or linked to terrorism. If you bought the argument that the AUMF included permission to conduct surveillance within the United States outside the bounds of FISA, the terms of Bush's content authorization lined up, more or less, with the language of the AUMF.

Metadata was another story, however. The point of looking at all that metadata was, as intelligence officials like to say, to gather a haystack so you could search for needles. Analyzing the metadata—the transactional information about a huge pool of phone and Internet communications—was supposed to help the NSA figure out which particular calls and e-mails they needed to be intercepting. Obviously, then, *that* bulk collection couldn't be limited to members of Al Qaeda and their allies.

Instead, the president's authorization allowed metadata collection for any communication with at least one end outside the United States, or for communications where no party was "known" to be a U.S. citizen. Clearly, though, it would be harder to rely on the AUMF as the authority for that collection. And for reasons I'll explain in a second, NSA may have had to analyze both domestic and foreign Internet traffic in many cases, just to sort out which was which.

For the phone records, this wasn't necessarily a big problem. Obtaining the phone company's business records—the "Call Detail Records" the carriers maintain anyway for their own business purposes—would not count as "electronic surveillance" as defined by FISA. Moreover, current (and widely criticized) Supreme Court doctrine holds that such business records are not protected by the Fourth Amendment. While other laws prohibit the disclosure of phone records to the government, they can be obtained without judicial approval via a National Security Letter or subpoena.

Even without those authorities, government lawyers may have concluded that the relevant laws didn't apply to the president's inherent authority in the intelligence arena. The FISA statute, after all, says that FISA and the Wiretap Act provide the "exclusive means" for governmental "electronic surveillance"—explicitly overriding any supposed inherent presidential authority. But it doesn't say that about things that *don't* qualify as "electronic surveillance," even when FISA has procedures in place to cover those other types of data collection.

Internet metadata, however, would have been trickier. To see why, it's important to understand how the Internet works differently from the phone network. When the phone company connects a call on a traditional circuit-switched phone network, it naturally has to know which two numbers it is connecting, and for how long—which is pretty much the sum of the relevant "metadata."

But that's not how a packet-switched network like the Internet works. Packets of Internet information don't just consist of "metadata" and "content," but of many levels of metadata at different "layers" of the OSI stack familiar to techies. The many computers or programs involved in routing and processing that data typically only need to "look" at one or two of those layers to do their job. Especially if it's just routing traffic from one foreign computer to another—traffic that just happens to be passing through the United States because that's the cheapest path—the company running an Internet backbone doesn't need to "see" or make any record of, for example, who is supposed to receive a particular e-mail or what Web page a user is trying to browse.

To oversimplify somewhat: The router essentially only needs to know the Internet Protocol address of the computer that's supposed to get a particular packet of data. If you send an e-mail to jsanchez@cato.org, the router doesn't really need to know that's what it's passing on: It sees that the packet is addressed to a particular port at 72.32.118.3 (the Cato Institute's IP address) and just forwards it along. Then it's up to Cato's servers to "look" deeper into the next layer of data and determine that, oh yes, it's an e-mail message that should be delivered to the user named jsanchez.

This is the essence of the "end to end" architecture of the Internet: The "pipes" carrying data can be relatively dumb, just moving data to the right destination server, and letting the server take things from there. And that IP-level metadata wouldn't even necessarily tell you whether the underlying communication was domestic or international. A packet of data traveling between Google's servers and Yahoo!'s, for instance, might actually be carrying a message from a Google user in Pakistan to

a Yahoo! user in Yemen.

What all of that means is that an company such as AT&T wouldn't necessarily have any "business records" that contain the kind of metadata the NSA was interested in. Instead, the NSA would have to sift through the entire traffic stream itself and pluck out the metadata (and content) that needed further analysis. It did so, as we know thanks to an AT&T whistleblower, in a series of secret rooms containing powerful "semantic analyzers" that filtered all the traffic flowing through the company's fiber optic cables.

That, however, would pretty clearly be "electronic surveillance" as defined by FISA, meaning it would require either a warrant or (if they just wanted the metadata) a pen register order from the secret FISA court. And since they wanted *everyone*'s metadata, not just that of suspected Al Qaeda operatives, they would have a harder time applying the "AUMF exception" theory for permission.

At first, according to the leaked NSA report, it seems like government lawyers tried to evade this rather obvious problem with variety of word games:

Specifically, NSA leadership, including OGC lawyers and the IG, interpreted the terms of the Authorization to allow NSA to obtain bulk Internet metadata for analysis because NSA did not actually "acquire" communications until specific communications were selected. In other words, because the Authorization permitted NSA to conduct metadata analysis on selectors that met certain criteria, it implicitly authorized NSA to obtain the bulk data that was needed to conduct the metadata analysis.

There were a couple of problems with this. First, while the NSA's own internal definitions may not count a communication as "acquired" until it has been processed into a human-readable form, that's not the definition that applies anywhere else in the law. Rather, if you bug someone's room or tap her phone, you've "intercepted" her communication (and committed a felony) as soon as it's rerouted into your recording device, regardless of whether you ultimately *listen* to the recorded conversation. As one federal court has put it, "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time."

Second, NSA lawyers hadn't actually been kept in the loop on the legal justifications for the program, which means they may not have understood that the administration was now relying on the AUMF as their authority for circumventing the FISA process. Maybe the words of the president's authorization could be stretched to permit initial bulk collection, but it would be much harder to make the argument that the language of the AUMF could be similarly stretched.

This, then, was almost certainly the problem that provoked the hospital showdown. The interception of phone and e-mail content was clearly electronic surveillance, but it was (in theory) limited to targets within the scope of the AUMF, which allowed the president to "determine" who had "aided" the 9/11 perpetrators. The bulk collection of phone records was not limited, but it also wasn't "electronic surveillance" as defined by FISA. The bulk collection of Internet metadata, however, was both plainly "electronic surveillance" and too broad to shoehorn into the language of the AUMF. Comey, it would seem, wasn't willing to countenance the legal gymnastics required to pretend otherwise.

Of course, we now know that the same data was soon being collected again under a blanket "pen register" order from the FISA Court—though the Court apparently imposed stricter limits on it than the NSA's own lawyers had. This particular type of bulk collection was reportedly halted in 2011.

What they're doing now instead is anybody's guess.

https://www.cato.org/blog/what-ashcroft-hospital-showdown-was-about