ars technica

What the Ashcroft "Hospital Showdown" on NSA spying was all about

How the government sought to justify blanket collection of Internet metadata

By: Julian Sanchez, *Senior Fellow at the Cato Institute* – July 29, 2013

We've known for years that the STELLAR WIND surveillance program—a massive NSA effort authorized by President George W. Bush after 9/11—eventually led to a dramatic showdown at the bedside of then-attorney general John Ashcroft. The situation surrounding STELLAR WIND was on such shaky legal ground that top members of the government threatened to quit in protest, though the exact reasons for their unease have been difficult to pinpoint.

Now, documents leaked by Edward Snowden have finally given us a clearer idea of what that showdown was really about: the wholesale collection of Internet metadata.

Showdown

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. Comey 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. Bush reauthorized the program despite the Justice Department's conclusion that it was unlawful. Comey then 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 program was briefly suspended, until it could be renewed under a different legal authority.

In 2008, we learned that the central bone of contention during this showdown wasn't warrantless wiretapping but rather some form of data mining. 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. The NSA report 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.

Data and metadata

STELLAR WIND had four components, each corresponding to types of information that President Bush 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 originally carried out this surveillance under the radical theory of "inherent presidential authority" spelled out by then-Justice Department lawyer John Yoo. The theory held that, during wartime, the president's surveillance powers could not be constrained by Congress or even by the Fourth Amendment. After Yoo 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.

Instead, 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 passing the AUMF, which suggests that Congress didn't think it already gave the president*carte blanche*. 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, this 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* (as opposed to metadata) 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.

It's different on the Internet

The point of looking at so much metadata is, as intelligence officials like to say, to gather a haystack so you can search for needles. Analyzing 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 collect, which meant that this metadata collection couldn't be limited to members of Al Qaeda and their allies.

Instead, the president's authorization allowed metadata collection on any communication with at least one endpoint outside the United States, or for communications where no party was "known" to be a US citizen. Clearly, though, it was harder to rely on the AUMF as the authority for that collection. And the 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" that 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 anyway. 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.

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. That's pretty much the sum of the relevant metadata.

But that's not how a packet-switched network like the Internet functions. 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 webpage a user is trying to browse.

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. And that's exactly what the agency did. We know that thanks to an AT&T whistleblower, who described a series of secret rooms containing powerful "semantic analyzers" that filtered all the traffic flowing through a company's fiber optic cables.

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

What to do, then?

Words and meanings

At first, according to the leaked NSA report, it seems government lawyers tried to evade this rather obvious problem through a variety of word games.

Specifically, NSA leadership interpreted the terms of the Authorization to allow NSA to obtain bulk Internet metadata for analysis because the NSA did not actually "acquire" communications

until specific communications were selected. In other words, because the Authorization permitted the NSA to conduct metadata analysis on selectors that met certain criteria, it implicitly authorized the 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 a 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 is 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 STELLAR WIND program, which means they may not have understood that the administration was now relying on the AUMF as the authority for circumventing the FISA process.

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 also 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.

This time, it's legal

Of course, we now know that after the hospital showdown, the administration simply went to the FISA court and obtained a blanket "pen register" order allowing the metadata collection to continue, this time with legal cover (though the Court apparently imposed stricter limits than the NSA's own lawyers did).

This particular type of bulk Internet metadata collection was reportedly halted in 2011. What the NSA is doing now instead is anybody's guess.