SECTION 215 ORDER REVEALS SECRECY ONLY SERVES TO PREVENT COURT CHALLENGE

Last March, when Hank Johnson asked him a poorly worded question about what NSA was doing with its data center in Utah, NSA head Keith Alexander kept saying the NSA had no power to collect in the US.

> Johnson: "NSA's signals intercepts include eavesdropping on domestic phone calls and inspection of domestic emails." Is that true?
>
> Alexander: No, not in that context. I think what he's trying to raise is are we gathering all the information on the United States? No, that is not correct.
>
> Johnson: What judicial consent is required for NSA to intercept communications and information involving American citizens?
>
> Alexander: Within the United States, that would be the FBI lead. If it was foreign actor in the United States the FBI would still have the lead and could work that with the NSA or other intelligence agencies as authorized. But to conduct that kind of collection in the United States it would have to go through a court order and a court would have to authorize it. We're not authorized to do it nor do we do it.

As I noted at the time, Alexander didn't actually deny it happens. He just said the FBI would have that authority in the US.

> Alexander never denies that such capabilities exist. Rather, he says that FBI would intercept communications—with

> a court order—and FBI would search for certain content—with a warrant.

I even pointed to the great deal of circumstantial evidence that the FBI uses Section 215 to do bulk collection.

> We know several things about the government's collection in the US. First, the telecoms own the equipment—they're the ones that do the intercepts, not FBI or NSA. Second, the FBI can and does get bulk data information from telecoms and other businesses using Section 215 of the PATRIOT Act.
>
> I will have more to say about this later—until then, read this post and this post as background.
>
> There is a great deal of circumstantial information to suggest that after the 2004 hospital confrontation—which was in part a response to Congress prohibiting any DOD use of data mining on Americans—chunks of the illegal wiretap program came to be authorized under Section 215 of the PATRIOT Act, which authorizes FBI data collection.
>
> There's nothing General Alexander said in this non-denial denial that would conflict with the notion that FBI collects data the telecoms intercept using Section 215 of the PATRIOT Act.

The Guardian's publication of a 215 Order collecting metadata from all of Verizon Network Business Services customers proves that I was correct. It proves that Alexander's obviously false non-denial was just that: a dodge of the truth.

Indeed, the order also shows that FBI's role is simply to provide legal cover by submitting the 215 request, but NSA gets the data.

The (anonymous, of course) Administration response to last night's disclosure is to claim it is no big deal.

> An administration official called the phone data a "critical tool in protecting the nation from terrorist threats to the United States."
>
> "It allows counter terrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, particularly people located inside the United States," the official added.
>
> [snip]
>
> "The order reprinted in the article does not allow the Government to listen in on anyone's telephone calls, said the administration official Thursday defending the decision. "The information acquired does not include the content of any communications or the name of any subscriber. It relates exclusively to metadata, such as a telephone number or the length of a call."

Note: congratulations to The Hill's Meghashyam Mali, who actually repeated this anonymous person's claim that 1) the program allows the government to ID terrorists but 2) the 215 Order does not return the ID of any subscriber, as if doing so constituted journalism. (Note: Marc Ambinder just posts the talking points, without noting how internally contradictory they are—I'll return to them shortly.)

Here's the question, though: if this program is no big deal, as the Administration and some members of Congress are already claiming in damage control, then why has the Administration been making thin non-denial denials about it for years? If it is so uncontroversial, why is it secret?

Is there anything about the order that tips people off to whom, precisely, is being targeted? Does it explain how good (or bad) NSA's data analysis tools are?

No. The collection is so broad, it could never provide hints of who is being investigated.

The WaPo suggests this order is just regular, routine collection, that quarterly 215 order sent to Verizon NBS. But even if, as I wondered last night, it's triggered to a specific investigation, is there anything in there that tells people what or who is being investigated?

No.

There is nothing operational about this Section 215 order that needs to be secret. Nothing. A TS/SCI classification for zero operational reason.

The secrecy has been entirely about preventing American citizens from knowing how their privacy had been violated. It serves the same purpose as Alexander's obviously dishonest answer.

And the most important reason to keep this secret comes from this claim, from the Administration's LOL talking points.

> As we have publicly stated before, all three branches of government are involved in reviewing and authorizing intelligence collection under the Foreign Intelligence Surveillance Act. Congress passed that act and is regularly and fully briefed on how it is used, and the Foreign Intelligence Surveillance Court authorizes such collection.

The Administration wants you to believe that "all three branches" of government have signed off on this program (never mind that last year FISC did find part of this 215 collection illegal — that's secret too).

But our court system is set up to be an

antagonistic one, with both sides represented before a judge. The government has managed to avoid such antagonistic scrutiny of its data collection and mining programs — even in the al-Haramain case, where the charity had proof they had been the target of illegal, unwarranted surveillance — by ensuring no one could ever get standing to challenge the program in court. Most recently in Clapper v. Amnesty, SCOTUS held that the plaintiffs were just speculating when they argued they had changed their habits out of the assumption that they had been wiretapped.

This order might just provide someone standing. Any of Verizon's business customers can now prove that their call data is, as we speak, being collected and turned over to the NSA. (Though I expect lots of bogus language about the difference between "collection" and "analysis.")

That is what all the secrecy has been about. Undercutting separation of powers to ensure that the constitutionality of this program can never be challenged by American citizens.

It's no big deal, says the Administration. But it's sufficiently big of a deal that they have to short-circuit the most basic principle of our Constitution.