

THE GOVERNMENT PLAYS CONNECT-THE- DOTS DIFFERENTLY THAN THEY SAY

In my continuing obsession to understand precisely how the government really uses the dragnet, consider this post, in which NSA Review Group member Geoffrey Stone conducts (IMO) inadequate analysis to conclude the phone dragnet is probably unconstitutional.

In it, he provides this description of how the government uses the phone dragnet:

In 2012, the NSA queried a total of 288 phone numbers. Based on these queries, the NSA found 16 instances **in which a suspect phone number was directly or indirectly in touch with another phone number that the NSA independently suspected of being associated with terrorist activity**. In such cases, the NSA turns the information over to the FBI for further investigation.

In terms of the “connect the dots” metaphor, the purpose of the program is not so much to discover new “dots” but to determine if there are connections between two or more already suspect “dots.” **For example, if a phone number belonging to a terrorist suspect in Pakistan is found to have called a phone number in the United States that the government independently suspects belongs to a person involved in possible terrorist activity**, alarm bells (figuratively) go off very loudly, alerting the government to the need for immediate attention. [my emphasis]

I don’t think this can be an accurate description of how the dragnet works.

It is close to what happened with Adis Medunjanin. As the FBI was honing in on Najibullah Zazi, the NSA did a query and found a new cell phone for Medunjanin, though they already knew Medunjanin was a likely accomplice of Zazi's through via travel records. The government says they were particularly interested in this phone because it was in contact with other extremists. Thus, they found a brand new phone number, but one that ended up being associated with both a suspect (Medunjanin) and other suspects (the other people that phone was in contact with).

But that cell phone for Medunajnin was a brand new number to the NSA, at least according to their reports.

The claim may still be true if they used burner matching to identify Medunjanin as a match to the other phone record they had on him. But it seems this process would have to involve additional information about Medunjanin at some point – at the very least, the match of those travel documents to that phone number, if not his identity.

In other words, this only seems to make sense if they had Medunjanin's "identity" in some form or another, belying their claims not to have identities while they're contact chaining.

The description is potentially more problematic with Basaaly Moalin. In his case, the stated explanation for what happened is they found his number on a second-degree search, sent it to the FBI, and the FBI learned he was the guy who had previously been investigated in 2003.

The problem might be alleviated in two ways: first, if the *hawala* through which Moalin was sending money to Ayro, was also tied to a suspect number. That's a distinct possibility: but the question is, how does that identity as a suspect number get communicated to NSA? If NSA already had it, doesn't it mean they've got more suspect numbers sitting somewhere than have been RAS approved?

The other possibility is that Moalin himself was still identified as a suspect number from the investigation back in 2003 – that an investigation that turned up no evidence might still, during the era of the illegal program, have gotten someone nominated as a suspect number under Cheney's program, and they never purged the system entirely (which would seem to be supported by the 2009 problems, which showed they hadn't turned off the illegal program features).

Either of these possibilities, of course, would raise new concerns about the NSA program.

But the description would also raise real issues, both about the honesty of witnesses and the potential efficacy of the system. If the NSA only triggers on people who've got ties to a second suspect number (which is entirely different than what they've been saying) then it could not possibly alert the government to a fully compartmented lone actor (someone like, say, Faisal Shahzad). That is, it would only find people who were engaged in the kind of elaborate planning seen before the government dismantled al Qaeda, but would not find the kind of individual extremists we've seen almost exclusively (with the exception of Zazi) for years.

This would answer the question of whether the NSA is finding the right numbers, in that it would be less likely to find someone innocent. It also might explain why the program didn't find Shahzad. But it would also mean it does (as presented) far less than the NSA has been saying it does.

I don't actually believe that, but that is what it would suggest.