NSA'S SINGLE SECTION 215 SUCCESS WOULD PROBABLY BE IMPOSSIBLE IF NSA'S LATEST CLAIMS WERE TRUE

It looks increasingly like the sole Section 215 success the FBI has had would be impossible under the claims about limits to dragnet collection NSA leaked last week.

Last week, four journalists reported that the NSA doesn't collect cell phone data in its phone dragnet program (they presumably meant, but did not specify, just the Section 215-authorized phone dragnet, which is just a small part of the phone dragnet). (WSJ, WaPo, LAT, NYT) As a result — these reporters claimed — as more and more Americans rely on cell phones, the NSA's phone dragnet has come to cover just 20 to 30% of the phone data in the US.

As I noted, the claim was particularly curious given that all the major examples in which the NSA has used the phone dragnet involved cell phone users.

Still, even in those cases, it was possible that NSA got the phone records via interim hops. That is, if a land line user whose calls were picked up in the dragnet called two cell phones, those numbers would be identified, though their calls to other cell users would not (again, this is if these recent claims are correct).

All that said, the sole case where the dragnet found someone with ties to terrorism they otherwise would not have identified, San Diego taxi driver Basaaly Moalin, increasingly looks to have been impossible under the terms now claimed by NSA leakers.

That's because Moalin and his known US-based interlocutor through whom the government says he communicated with Somali warlord Aden Ayro, *hawala* operator Mohamed Ahmed, both used cell phones, both from T-Moble, according to Moalin's attorney Joshua Dratel. The government has said it identified Moalin on at least the second hop. If that interim hop was Ahmed, Ahmed's calls to Moalin would not have been collected, if the NSA's current claims are true.

Assuming Ahmed was that interim hop, then, the dragnet could not have identified Moalin, at least not under the limits currently claimed by the NSA and the public claims made about the investigation into Moalin.

There are several possible explanations for why the phone dragnet did find him.

First, it's possible the claims are entirely false, and that the NSA includes T-Mobile in its Section 215 collection. I think that's unlikely; for a variety of reasons I believe just 3 providers — AT&T, Verizon, and Sprint — get Secondary Orders under the phone dragnet.

It's possible that an earlier WSJ story (cited by several of these reporters) correctly described how T-Mobile data gets included in the dragnet: via the backbone provider of the networks T-Mobile uses (which, if claims Verizon doesn't provide cell data are true, would mean AT&T provided it).

> The National Security Agency's controversial data program, which seeks to stockpile records on all calls made in the U.S., doesn't collect information directly from T-Mobile USA and Verizon Wireless, in part because of their foreign ownership ties, people familiar with the matter said.
>
> The blind spot for U.S. intelligence is relatively small, according to a U.S. official. Officials believe they can still capture information, or metadata, on 99% of U.S. phone traffic because

> nearly all calls eventually travel over
> networks owned by U.S. companies that
> work with the NSA.
>
> [snip]
>
> When a T-Mobile or Verizon Wireless call
> is made, it often must travel over one
> of these networks, requiring the carrier
> to pay the cable owner. The information
> related to that transaction—such as the
> phone numbers involved and length of
> call—is recorded and can then be passed
> to the NSA through its existing
> relationships. Additionally, T-Mobile
> relies on other wireless companies to
> fill holes in its infrastructure. That
> shared equipment could allow the
> government to collect the data.

If that's the case, however, it means the only way the current claims about the Section 215 dragnet are true is if this collection happens offshore, counting as EO 12333 collection. Which would further mean that even with 20% coverage from domestic production, the NSA still gets most calls in the US.

Finally, it's possible the dragnet identified Moalin via collection entirely collected overseas. Which would mean the claims he was identified under Section 215 — made repeatedly to Congress (though not, curiously, in declarations in the lawsuits against the dragnet) — would be false. It would also mean his prosecution was based on the foreign collection of US person data under no more than an Executive Order.

Here's the remarkable thing about those two last possibilities. At least as late as March 2009, the NSA could not distinguish the data source for its dragnet query results. A query result from October 2007, when Moalin was first identified, might not distinguish between EO 12333 and Section 215 in the results — though at least according to FISC orders, the Section 215

data may not have gotten mixed in with the EO
12333 data yet. (By 2011, results came back
tagged with XML tags to identify not only what
authority the data was collected under, but
which SIGAD collection point it had been
collected from, though some data points get
collected under more than one authority and
collection point.) That means, unless NSA knows
for a fact how it collected T-Mobile data back
in 2007, it may not know how it found Moalin.
And if it found Moalin off an EO 12333 search,
NSA would not have needed even Reasonable
Articulable Suspicion to search for connections.
It is possible that if NSA initiated the search
on any Somali but Aden Ayro (Ayro had ties with
Al Qaeda beyond just his al-Shabaab membership
and therefore would meet RAS guidelines), they
would not have had Reasonable Articulable
Suspicion that the identifier had ties to Al
Qaeda.

In any case, as I laid out, there are a number
of ready explanations for how the dragnet
identified Moalin even though he and one likely
intermediary were using phones purportedly not
collected under the dragnet. But those
explanations either mean the recent claims about
the extent of the dragnet collection are false,
or there are many more questions about how
Moalin got targeted.