THE NSA DOES KNOW THE IDENTITY OF SOME OF THE TARGETS IT IS CONTACT-CHAINING

One claim the NSA has made just about every time one of its representatives has talked about the phone dragnet is that, because the dragnet contains only phone numbers, analysts don't know who they're chaining on. They have to give a number to the FBI, NSA people claim, where they use "additional legal process" to find the identity (more on that later).

And that may be true … up to a point.

But the claim goes far beyond even what the NSA (with an assist from friendly media partners) depicts.

Consider 60 Minutes depiction of of contact chaining (at 2:36).

> Analyst Stephen Benitez showed us a technique known as "call chaining" used to develop targets for electronic surveillance in a pirate network based in Somalia.
>
> Stephen Benitez: As you see here, I'm only allowed to chain on anything that I've been trained on and that I have access to. Add our known pirate. And we chain him out.
>
> John Miller: Chain him out, for the audience, means what?
>
> Stephen Benitez: People he's been in contact to for those 18 days.
>
> Stephen Benitez: One that stands out to me first would be this one here. He's communicated with our target 12 times.
>
> Stephen Benitez: Now we're looking at

> Target B's contacts.
>
> John Miller: So he's talking to three or four known pirates?
>
> Stephen Benitez: Correct. These three here. We have direct connection to both Target A and Target B. So we'll look at him, too, we'll chain him out. And you see, he's in communication with lots of known pirates. He might be the missing link that tells us everything.
>
> John Miller: What happens in this space when a number comes up that's in Dallas?
>
> Stephen Benitez: So If it does come up, normally, you'll see it as a protected number– and if you don't have access to it, you won't be able to look.
>
> If a terrorist is suspected of having contacts inside the United States, the NSA can query a database that contains the metadata of every phone call made in the U.S. going back five years.

Working solely at the level of identifier, the software alerts him whether the first and second-degree contacts are "known pirates." Given that the analyst is working on EO 12333 collected data, these targets do not have to have been reviewed for Reasonable Articulable Suspicion that they are pirates. But the system identifies them as such.

And, while this is more subtle, Benitez at least portrays the chaining process to move immediately onto "known Target B," suggesting he may recognize precisely who that pirate is upon seeing the identifier.

I mocked the 60 Minutes piece for – among other things – showing us EO 12333 contact chaining to allay our concerns about the Section 215 phone dragnet.

But even with Section 215 dragnet, the NSA itself admits analysts might immediately

recognize the identity of those they are contact chaining. This passage appears in one of their training programs on the process (see page 20).

> So, for example, if you run a BR or PR/TT query on a particular RAS-approved e-mail identifier and it returns information that depicts identifier A, the RAS-approved see, was in direct contact with identifier B and the source of the metadata is BR or PR/TT, then just the fact that identifier A is communicating with identifier B is considered a BR or PR/TT query result.
>
> [snip]
>
> So if you knew that identifier A belonged to Joe and Identifier B belonged to Sam, and the fact of that contact was derived from BR or PR/TT metadata, if you communicate orally or in writing that Joe talked to Sam, even if you don't include the actual e-mail account or telephone numbers that were used to communicate, this is still a BR or PR/TT query result.

To guard against an analyst immediately telling colleagues who aren't phone dragnet cleared, the NSA makes it clear she shouldn't just call them and say Joe and Sam have been chatting.

That risk exists because the analyst "knew that identifier A belonged to Joe and Identifier B belonged to Sam" — she knew who she was chaining off of.

This is not all that surprising. If you work with a phone number or email address enough, you're going to recognize it as the identity of the person who uses it.

Yet it does suggest analysts get enough context — either through the target identifiers they use to target someone in the first place, or from accessing the content of the communications they chain off of — to "know" the identities of some

the people that come up in contact chains.

We would expect them to have this context. It surely makes their analysis better informed.

But given that they do have this context, it is completely misleading for the NSA to claim they don’t know the identity of the people they’re contact chaining.