THE GOVERNMENT'S UNEXPLAINED IRAN DRAGNET

Just the other day, I observed that the government likely has a problem with the authorities it has used to police its sanction regime against Iran. First, the government appears to have had a counterproliferation certification under Protect America Act that may have had legal issues; with FISA Amendments Act, Congress authorized such a certification as foreign intelligence. Then, at some point over the course of the phone dragnet, FISC approved the use of the dragnet with Iran under an alleged terrorism purpose. But the primary claimed Iranian terrorism in this country was propagated by DEA; clearly the NSA was using the dragnet for an inherently counterproliferation purpose.

A judge in DC just ruled for the government in a case against an Iranian American, Shantia Hassanshahi, that implicates many of these problems, and broader problems with the dragnet, though he did so by largely sidestepping the underlying issue.

Basically, the case that Hassanshahi violated sanctions stems from the following evidentiary steps:

1. An unsolicited tip from an (apparently) paid informant
2. A query request submitted to some unnamed database on a suspect number, which returned a single call with a number associated with Hassanshahi
3. Based on that and 1 other call to Iran, the government

stopped Hassanshahi as he returned from a trip to Iran and seized his devices in CA

4. A forensic search of his laptop resulted in incriminating documents showing the sale of non-military energy-related goods to Iran

Hassanshahi argued that the query of the database – which he argued was either the phone dragnet database or something nearly identical and therefore just as unconstitutional – was illegal, citing Richard Leon's Larry Klayman ruling. And he argued that everything else not only followed as fruit of the poison tree from there, but that the device search violated the 9th Circuit's precedent requiring probable cause to conduct a forensic border search (his devices were seized in CA, not in DC). Judge Rudolph Contreras rejected Hassanshahi's bid to have the evidence suppressed by dodging the question of the legality of the database query, treating it as unconstitutional (I think this overstates what the government was saying here).

> In response, the Government sidesteps Hassanshahi's argument by taking the position that although the NSA telephony database was not used, the Court nevertheless should assume arguendo that the law enforcement database HSI did use was unconstitutional. See Gov't's Mem. Opp'n Mot. Suppress 12. Consistent with this position, the Government refuses to provide details about its law enforcement database on the basis that such information is irrelevant once the Court accepts the facial illegality of the database. See id. at 11-12. Regrettably, the Court therefore starts its analysis from the posture that HSI's initial search of the mysterious law enforcement database, which uncovered

> one call between Sheikhi's business telephone number and the 818 number linked to Hassanshahi, was unconstitutional

But based on the time that elapsed between the query he treated as unconstitutional and the border search, and based on Hassanshahi's voluntary arrival in LAX (where a 9th Circuit ruling would require reasonable suspicion) and some really crazy details even the government didn't argue that strongly constituted reasonable suspicion, he ruled the forensic search in LA legal.

This is where things get bizarre. Having already ruled that this was not flagrant enough to make the subsequent search improper, Contreras then throws up his hands, notes that if the government did use the NSA phone dragnet (which is supposed to be limited to counterterrorism purposes and therefore should be inapplicable in this case) or if the dragnet it used doesn't have the controls that the NSA dragnet does it might be a problem, he says he will require the government to submit an ex parte filing explaining the database.

> But, at the same time, the Court does not know with certainty whether the HSI database actually involves the same public interests, characteristics, and limitations as the NSA program such that both databases should be regarded similarly under the Fourth Amendment. In particular, the NSA program was specifically limited to being used for counterterrorism purposes, see Klayman, 957 F. Supp. 2d at 15-16, and it remains unclear if the database that HSI searched imposed a similar counterterrorism requirement. If the HSI database did have such a limitation, that might suggest some level of flagrancy by HSI because it was clear that neither Sheikhi nor Hassanshahi was involved in terrorism activities. With

> so many caveats, the Government's litigation posture leaves the Court in a difficult, and frustrating, situation. Yet, even assuming that the HSI database was misused to develop the lead into Hassanshahi, HSI's conduct appears no more flagrant than law enforcement conduct in other "unlawful lead" cases,which still held that the attenuation exception applied nonetheless.6
>
> 66 The Government's silence regarding the nature of the law enforcement database has made the Court's analysis more complex than it should be. Although the Court still concludes that the attenuation exception applies in large part based on the "unlawful lead" line of cases, the Court will order that the Government provide the Court with an ex parte declaration summarizing the contours of the mysterious law enforcement database used by HSI, including any limitations on how and when the database may be used.

Of course he only requires this after ruling that the evidence can come in!

Now, I can think of four possibilities to explain the search:

- The government searched the dragnet under its "Iranian" allowance (which only Josh Gerstein and I have ever reported), exposing what I noted above — that they're using a CT tool for a fundamentally CP function
- The government searched Hemisphere
- The government searched

SPMCA, the authority permitting it to contact-chain on US person data collected under EO 12333 or it originally searched on the Section 215 phone dragnet then re-ran the search under EO 12333 so it could share the link
- There's yet another dragnet

Something's definitely fishy about the government's claims, because the Homeland Security investigator in the case, Joshua Akronowitz changed his story twice in meaningful ways.

For example, the affidavit the government used to justify his arrest said he personally searched "HSI accessible law enforcement databases." But in an affidavit submitted with the government response to this motion, he said he "sent a research request for information," which is what other agencies would do with the NSA dragnet (though also, in some cases, with Hemisphere). That's important because as the defense noted in their reply,

> The government actually presents no evidence that the database is not the NSA database. The government makes this claim in its memorandum, but there is nothing in the affidavit. Attorney argument in the memorandum is not evidence.'

Akronowitz' story also changed about how many calls to Iran were returned in his search of the database. In his initial affidavit, Akronwitz claimed he found "a number of telephone calls" between Hassanshahi and the target of the query. In his second one, Akronowitz said he found a call "on one occasion," but after he subpoenaed Google for Hassanshahi's call records, he found

"numerous phone calls" between Hassanshahi's number and a different Iranian number. In yet a third affidavit, Akronowitz stuck with the single call between the target and Hassanshahi's number, but then admitted that Hassanshahi's number reflected "contact with [the other] Iranian phone number … only once," while also claiming a call to 22932293 was also an Iranian number.

I would suggest this changing story likely arises from the need to hide how long records were kept in the database in question, and possibly the use of 2-hop searches (which would find the second Iranian number). And the claim that the third number is Iranian likely reflects another kind of record, which I'll get to in coming days.

That is, I think Akronowitz may be making shit up to hide features about the database he is trying to hide.

There's one other important detail, one which leads me to suspect this is a search of SPCMA data. The LA-based Hassanshahi number in question is a Google voice number, not a cell phone and not a landline. Also, Akronowitz' story about how he found that it was a Google number changed over the affidavits too. We keep hearing that the phone dragnet increasingly includes a smaller percentage of US calls, missing both cell phone numbers and VOIP. It would also only show up in a Hemisphere search if it cross an AT&T backbone (though that's possible). That Hassahshahi was found in a database — whichever it was — that includes both VOIP and land lines makes his argument under the Maynard precedent even stronger, because it suggests they're chaining across technologies.

The government is clearly trying to hide additional details about this dragnet — whether it's the fact they use it against Iranian counterproliferation targets, whether it's that Hemisphere is used for more than drug targets, whether it's that they're chaining on foreign collected data. And sadly, Contreras has deemed

it legal before requiring the government to explain what the hell it is trying to hide.