RAEZ QADIR KHAN: HOISTING THE FBI ON ITS OWN METADATA PROBLEMS

Type	2005	2006	2007	2008	2009	2010	2011	2012	2013
Phone content									
Email content									
Cell phone content					September	January			
FedEx intercept					November				
Misc records									
Credit reports					September				
Wire transfers									
Call detail records									
Internet searches									
Bank records								September	
Residence									March

As I said earlier, the lawyers defending Pakistani-American Raez Qadir Khan – who is accused of material support of terrorist training leading up to an associate's May 2009 attack on the ISI in Pakistan – are doing some very interesting things with the discovery they've gotten.

Request for Surveillance Authorities

The first thing they did, in a July 14, 2014 filing, was to list all the kinds of surveillance they've been shown in discovery with a list of possible authorities that might be used to conduct that surveillance. The motion is an effort to require the government to describe what it got how.

The table above is my summary of what the motion reveals and shows only if a particular kind of surveillance happened during a given year; it only gives more specific dates for one-time events.

The brown (orange going dark!) reflects that emails were turned over in discovery from this period, but that the 2013 search warrant apparently says "authorization to collect emails existed from August 2009 to May 2012." That's not necessarily damning; they could get those earlier emails legitimately via a number of

avenues that don't involve "collecting" them. But it is worth noting for reasons I explain below.

The filing itself includes tables with more specific dates, Bates numbers, possible authorities, and — where relevant — search warrant items reliant on the items in question. It also describes surveillance they know to have occurred — further Internet and email surveillance, for example, a 2009 search of Khan's apartment, as well as surveillance in later 2012 — that was not turned over in discovery.

Effectively, the motion lays out all the possible authorities that might be used to collect this data and then makes very visible that the criminal search warrant was derivative of it (there's a bit of a problem, because the warranted March 2013 search actually took place after the indictment, and so Khan's indictment can't be entirely derivative of this stuff; that relies largely on emails).

I also think some of the authorities may not be comprehensive; for example, the pre-2009 emails may have been a physical FISA search. We also know FISC has permitted the government to collect URL searches under Section 215.

But it's a damn good summary of the multiple authorities the government might use to obtain such information, by itself a superb demonstration of the many ways the government can obtain and parallel construct evidence.

The filing seems to suggest that the investigation started in fall 2009, some months after Khan's alleged co-conspirator, Ali Jalil, carried out a May 2009 suicide attack in Pakistan. If that's right, then the government obtained miscellaneous records (which is not at all surprising; these are things like immigration and PayPal records), email content, and call detail records retroactively. Alternately (Jalil was arrested in the Maldives in April 2006 and interrogated by people

presenting themselves as FBI), the government conducted all the other surveillance back to 2005 in real time, but doesn't want to show Khan's team it has. In a response to this motion, the government claims that when the surveillance of Khan began is classified.

The motion for a description of which authorities the government used to obtain particular information is still pending.

Motion to Throw Out the Emails

Here's where things get interesting.

On September 15, Khan's lawyers submitted a filing moving to throw out all the email evidence (which is the bulk of what has been shown so far and — as I said — most of what the indictment relies on). It argues the 504 emails provided in discovery — spanning from February 2005 to February 2012—lack much of the metadata detail necessary to be submitted as authenticated evidence. Some of the problems, but by no means all, stem from FBI having printed out the emails, hand-redacted them, then scanned them and sent them as "electronic production" to Khan's lawyers.

That argument is highly unlikely to get anywhere on its own, though a declaration from a forensics expert does raise real questions about the inconsistency of the metadata provided in discovery.

But the filing does pose interesting questions that — in conjunction with questions about the authorities used to investigate Khan — may be more fruitful.

First, there's FBI's computer limitations. You'll recall that one of probably several reasons why the FBI refuses to count its back door searches is because it stores traditional FISA and 702 data in the same database and claims to be unable to install tracking easily. Khan received both traditional FISA notice

(when he was arrested) and FISA 702 notice (over a year later), so both authorities are at issue in this case. The filing invokes a related problem: FBI's Data Warehouse System (DWS) — described in some detail in the Webster report on the Nidal Hasan attack publicly released in 2012, which the filing cites, and almost certainly the database that FBI says can't track back door searches — has a limited ability to maintain and process huge amounts of information.

Former FBI Director William Webster says FBI's computer systems suck (which FBI says itself, when it serves its purposes), and this filing uses that to argue the emails stored in it are therefore unreliable.

Then there are details displayed by the various fields associated with some (but not all) of the emails provided in discovery. In an appendix, Khan's lawyers provide 10 (actually, 2 appear to be duplicates) emails to demonstrate the points they make about unreliability. In addition to metadata inconsistencies, they point to redactions of several FBI fields, which may be whim or may serve to hide relevant information. Here's a summary of what they show (I've included only the last name of the non-commercial emails for privacy reasons; click to enlarge).

Email	Date	DWS	Facility	Authority
[Latsher] to reaz2000@yahoo.com	11/5/07	Yes	Redacted	FISA
[Munahaque] to reaz2000@yahoo.com	7/16/10	Yes	reaz2000@yahoo.com	Redacted
[Latsher] to reaz2000@yahoo.com (apparent dupe of 1)	11/5/07	Yes	Redacted	FISA
info@aqratravel.com to reaz2000@yahoo.com	8/27/09	No	NA	NA
[tawab] to reaz2000@yahoo.com	12/31/09	Yes	Redacted	FISA
info@aqratravel.com to reaz2000@yahoo.com (apparent dupe of 4)	8/27/09	No	NA	NA
reaz2000@yahoo.com to info@aqratravel.com (key metadata missing)	12/24/08	Yes	Redacted	FISA
reaz2000@yahoo.com to [Sohail]	8/11/09	Yes	reaz2000@yahoo.com	Redacted
reaz2000@yahoo.com to [Ideal]	3/11/08	Yes	reaz2000@yahoo.com	Redacted
reaz2000@yahoo.com to [Malaak]	11/15/08	No	NA	NA

"Facility," remember, is FISA-speak for "target." So this seems to reflect Khan's own emails coming up in FISA targeted collection with a 2008 date, before the more active investigation appears to have started (though again, that could be a search of stored email). It also seems to show Khan's emails coming up in

FISA targeted collection targeting at least two other people, one of which targeted a Yahoo to Yahoo conversation from before Yahoo complied with Protect America Act (though if this was traditional FISA, that would be unsurprising). One of the emails that seems to be from Khan-targeted collection has its authority hidden, which may be more randomness or may reflect additional authorities used to collected US person email content.

In other words, the metadata the FBI has provided and declined to provide may say some interesting things about the investigation, which used both traditional and 702 FISA.

Then there are 2 emails that appear not to have been printed out from FBI's DWS, though they do have product numbers consistent with the DWS product numbers. Because they were printed out outside of the DWS system, they lack the header information pertaining to facility and authority of the email. Of note, both emails involving Aqra Travel appear to have had some funkiness which ended up hiding key details about whom Khan was communicating with at that apparent travel agency. Maybe they're hiding that the travel agency is really in Quantico?

The filing presents these redactions as haphazard (it even cites one email turned over in illegible form early in discovery, with the authority redacted, and the same email provided later in more legible discovery, with the authority unredacted), which they may well be. But if they serve to hide that collection was targeted at someone besides Khan under other authorities, it would serve to hide the extent to which FBI built its case against Khan using back door searches on other FISA-related collection.

FBI's Problem: Timing and "Collection"

Ultimately, I think these two filings together may present two problems for the government

(though remember, the judge in this case, Michael Mosman, is a FISA Court judge who refused to recuse himself on those grounds).

First, the government has a timing problem (rather, two). As I laid out above, it looks as if this investigation into Khan started in the aftermath of Jalil's suicide attack. Perhaps the government used the phone or Western Union dragnet to identify Jalil's US associates, found Khan, and used that metadata to pull up Khan's emails with Jalil using Section 702, which then provided the basis for a FISA warrant to investigate Khan directly. But that would amount to wiretapping a dead man to read an American's emails — which would seem to qualify as reverse targeting, which is forbidden under Section 702.

Alternately, the government was wiretapping Jalil at least as early as American authorities interviewed him in 2006, and either tracked Khan through his side of those communications or they identified Khan after Jalil's attack and then pulled up already-collected emails. But if they were wiretapping Jalil communications with US persons in 2006 — including a Yahoo account — then they may have been wiretapping Jalil under Stellar Wind. Which would make Khan an aggrieved person for illegal wiretapping under FISA. Khan's lawyers have been very diligent about laying a ground work for undisclosed EO 12333 collection.

Either way, answering these questions may provide Khan a way to challenge his prosecution, which relies heavily on the emails in question.

Then there's a collection problem. As the forensics expert hired by Khan's legal team lays out, there's a really easy way to solve the authentication problems of the emails turned over to Khan.

> It is my belief that much of the above noted issues regarding the lack of ability to search, sort, and even read the government provided documents

> could be alleviated if the original electronic documents were provided in their native format(s) to the defense.

But not only would that reveal information the government may not want to reveal to Khan (such as where that seeming travel agency really is). But they may not be able to provide all that information, because it doesn't exist anymore and instead only exists in a database that — even the FBI agrees, when it suits the Bureau — is a dysfunctional database not up to the task of storing data with integrity.

The point is that the problems behind authenticating most of the emails (aside from the ones that may not come from FBI's database) all stem from the fact that the government has conflated "collecting" and "searching" and the means they have of accomplishing that — FBI's DWS — introduces potentially legitimate questions about authentication.

Who knows whether this effort will serve to make that distinction legally problematic or not? But it seems to target a number of the constitutional problems with the current FISA regime via the currently awful means of implementing that regime.