

JUDGE PAULEY'S DELIBERATE BLIND SPOT: SYSTEMATIC SECTION 215 ABUSES

Sorry for my silence of late, particularly regarding William Pauley's ruling finding the phone dragnet legal. The good news is my mom can now reach the light switch in her sewing room without risk of falling.

As noted, Judge Pauley ruled against the ACLU in their suit challenging the phone dragnet. A number of commentators have pointed to some bizarre errors or focus in Pauley's ruling, including,

- Pauley says the government could not find the "gossamer threads" of terrorist plotters leading up to 9/11. They did find them. They simply didn't act appropriately with them.
- He unquestioningly considers the 3 uses of Section 215 (with Zazi, Headley, and Ouazzani) proof that it is effective. He does not note that even Keith Alexander has admitted it was only critical in one case, one not even mentioned in the government's filings in this case.
- He ignores the role of the Executive in willingly declassifying many details

this program, instead finding it dangerous to allow the ACLU to sue based on an unauthorized leak. The government has actually been very selective about what Snowden-leaked programs they've declassified, almost certainly to protect even more problematic programs from legal challenge.

- He claims Congress has renewed Section 215 7 times (including 2001, it was renewed it 5 times).
- He claims there is no doubt the Intelligence and Judiciary Committees knew about the rulings underlying the program in spite of the fact that some rulings were not provided until after Section 215 was renewed; he admits that the limits on circulation of notice in 2011 was "problematic" but asserts the Executive met its statutory requirements (he doesn't deal with the evidence in the record that the Executive Branch lied in briefings about the conduct of the dragnet).

There are also Pauley's claims about the amount of data included – he says the government collects all phone metadata; they say NSA collects far less data. This is a more

complicated issue which I'll return to, though maybe not until the New Year.

But I'm most interested in the evidence Pauley points to to support his claim that the FISC (and Congress) conduct adequate oversight over this program. He points to John Bates' limits to the government's intentional collection of US person data via upstream collection rather than Reggie Walton's limits to Section 215 abuses.

For example, in 20011, FISC Judge Bates engaged in a protracted iterative process with the Government—over the Government's application for reauthorization of another FISA collection program. That led to a complete review of that program's collection and querying methods.

He then immediately turns to Claire Eagan's opinion reiterating that the government had found and dealt with abuses of the phone dragnet program.

In other words, for some bizarre reason he introduces a series of rulings pertaining to Section 702 – and not to Section 215 – to support his argument that the government can regulate this Section 215 collection adequately.

It's particularly bizarre given that we have far more documents showing the iterative process that took place in 2009 pertaining directly to the phone dragnet. Why even mention the Bates rulings on upstream collection when there are so many Reggie Walton ones pertaining directly to Section 215?

I suspect this is because Pauley relies so heavily on the adequacy of the minimization procedures imposed by the FISC, as when he cites Claire Eagan's problematic opinion to claim that without adequate minimization procedures, FISC would not approve Section 215 phone dragnet orders.

Without those minimization procedures,

FISC would not issue any section 215 orders for bulk telephony metadata collection.

(Note, Pauley doesn't note that the government has not met the terms of the Section 215 itself with regards to minimization procedures, which among other things would require an analysis of the NSA using a statute written for the FBI.)

The only way Pauley can say the limits he points to in his analysis – that NSA can only analyze 3 hops deep, that FBI only gets summaries of the queries, that every query got approved for RAS – is if he ignores that for the first 3 years of the program, all of these claims were false.

He uses similar analysis to dismiss concerns about the power of metadata.

But [ACLU's contention that the government could use metadata analysis to learn sensitive details about people] is at least three inflections from the Government's bulk telephony metadata collection. First, without additional legal justification—subject to rigorous minimization procedures—the NSA cannot even query the telephony metadata database. Second, when it makes a query, it only learns the telephony metadata of the telephone numbers within three “hops” of the “seed.” Third, without resort to additional techniques, the Government does not know who *any* of the telephone numbers belong to.

These last assertions are all particularly flawed. Not only have these minimization procedures failed in the past, not only has the government been able to go four hops deep in the past (which could conceivably include all Americans in a query), not only is there abundant evidence – which I'll lay out in a future post – that the government does know the identities of at least some of those whom it is

chaining, but there are two ways the government accesses this data for which none of this is true: when “data integrity analysts” fiddle with the data to prepare it for querying, and when it is placed in the “corporate store” and analyzed further.

All the claims about minimization Pauley uses to deem this program legal have big big problems.

The NSA conducted a fraud on the FISC for 3 years (and still is, to the extent they claim the violations under the program arose from complexity rather than their insistence on adopting all the practices used under the illegal program for the FISC-authorized program). Yet Pauley points to the FISC to dismiss any Constitutional concerns with this program.

And to do that, he ignores the abundant evidence that all his claims have been – and may still be, in some cases – false.

JAMES CLAPPER CLAIMS PUBLICLY ACKNOWLEDGED DETAILS ARE STATE SECRETS WHILE BOASTING OF TRANSPARENCY

Between documents leaked by Edward Snowden, official court submissions, and official public statements, we know at least the following about the surveillance system set up after 9/11 and maintained virtually intact to this day:

- Around of 8-14% of the content collected under Bush's illegal program was domestic content (page 15 of the NSA IG Report says this constituted 8% of all the illegal wiretap targets but the percentage works out to be higher)
- Some of the content collected via ongoing upstream collection currently includes intentionally-collected domestic content (NSA refuses to count this, even for the FISA Court)
- Bush's illegal wiretap program targeted Iraqi Intelligence Service targets, as well as targets affiliated with al Qaeda and its associates (see page 8)
- NSA uses the phone metadata program with Iranian targets, as well as targets affiliated with al Qaeda and its associates
- Both the illegal wiretap program and the Internet dragnet authorized under Pen Register/Trap and Trace in 2004 collected information that (because of the way TCP/IP works) would be legally content if treated as electronic surveillance

- The NSA still conducts an Internet dragnet via collection overseas, which not only would permit the metadata-as-content collection, but would permit far more collection on US persons; that collection is seamlessly linked to the domestic dragnet collection
- NSA uses the dragnets to decide which of content the telecoms have briefly indiscriminately collected to read

That is, the surveillance system is not so much discrete metadata programs and content programs directed overseas, directed exclusively against al Qaeda or even terrorists. Rather, it is a system in which network analysis plays a central role in selecting which collected content to read. That content includes entirely domestic communication. And targets of the system have not always been – and were not as recently as June – limited to terrorists.

These details of the surveillance system – along with the fact that AT&T and Verizon played the crucial role of collecting content and “metadata” off domestic switches – are among the details James “Least Untruthful” Clapper, with backup from acting Deputy Director of NSA Frances Fleisch, declared to still be state secrets on Friday, in spite of their public (and in many cases, official) acknowledgement.

In doing so, they are attempting to end the last remaining lawsuits for illegal wiretapping dating to 2006 by prohibiting discussion of the central issue at hand: the government has repeatedly and fairly consistently collected the content of US persons from within the US, at

times without even the justification of terrorism. (For more background on Jewel v. AT&T, see here.)

Here's how Clapper, with a nod to Fleisch, lays out the rebuttal of the Jewel plaintiffs.

the NSA's collection of the content of communications under the TSP was directed at international communications in which a participant was reasonably believed to be associated with al-Qa'ida or an affiliated organization. Thus, as the U.S. Government has previously stated, plaintiff's allegation that the NSA has indiscriminately collected the content of millions of communications sent or received by people inside the United States after September 11, 2001, under the TSP is false.

There are several weasel parts of this claim.

The "Terrorist Surveillance Program" and the "Other Target Surveillance Program"

First, to make this claim, Clapper (and Fleisch) revert to use of "Terrorist Surveillance Program," a term invented to segment off the part of the larger illegal wiretap program that George Bush was willing to confess to in December 2005, that involving international communications with a suspected al Qaeda figure. But as Fleisch admits – but doesn't explain – at ¶20, the TSP is just a subset of the larger Presidential Surveillance Program. As I've noted above, we know the system was used and is currently used to target entities that are agents of states, not terrorist organizations. And Clapper's language suggests it is used with both "other foreign terrorist organizations" and to identify "many other threats."

...and other foreign terrorist organizations to the United States
[snip]

to the extent classified information about the al-Qa'ida threat, from September 11, 2001 to the present, or the many other threats facing the United States,

Given the evidence that the program may (or may have) extend beyond even the Iranian and Iraqi targets the government has deemed "terrorists" so as to include them in this program, Jewel's plaintiffs might be able to argue it could include normal dissent.

The Internet metadata that is really content

Then the government hides details that would make it clear that both under Bush and Obama, NSA illegally collected US person content in the name of collecting "metadata."

The first tell here is how Clapper refers to the "metadata" collected under Bush (this carries over into the I Con's announcement of this declassification).

President Bush authorized the NSA to collect (1) the contents of certain international communications, a program that was later referred to and publicly acknowledged by President Bush as the Terrorist Surveillance Program (TSP), and (2) **telephony and Internet non-content information (referred to as "metadata")** in bulk, subject to various conditions. [my emphasis]

While his reference varies, the emphasis on "non-content information (referred to as 'metadata')" suggests they're using a potentially uncertain definition of metadata.

This likely derives from the government's definition of content here. Both Clapper (footnote 1) and Fleisch (footnotes 4 and 11) note their discussion of the Internet "metadata" program defines content as defined under the pen register part of FISA. Here's Fleisch:

The term “content” is used herein to refer to the substance, meaning, or purport of a communication, as defined in 18 U.S.C. § 2510(8), as distinguished from the type of addressing or routing information referred to herein as “metadata.”

While they claim to be using “meaning” to distinguish from “metadata,” both are also implicitly distinguishing this definition of content used in the pen register statute from that used for electronic surveillance, which is,

“Contents”, when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

At one level, this is just tautological game-playing. The method the NSA used to collect the domestic Internet dragnet until December 2011 was exactly the same as it used for the Section 702 upstream collection, collection, with some filtering, directly from AT&T and Verizon’s switches; there is nothing in the **method** that distinguishes the Internet dragnet from what NSA treats as electronic surveillance of Internet content. So to define one object of collection as metadata and the other as content, they simply apply different definitions of content to them.

Moreover, there is long-standing legal awareness of this problem. Colleen Kollar-Kotelly relied on the pen register definition on page 6 of the original dragnet opinion. But with it, she required that collection be limited to certain kinds of metadata, a requirement that we know NSA violated from the very start.

John Bates laid out the problems with adopting the pen register definition generally and

therefore its definition of content specifically on pages 26 and following of his opinion authorizing the resumption of the Internet dragnet. That problem appears to pertain to the fact that the NSA was claiming that PR/TT allowed it to collect “dialing, routing, addressing, or signaling information” (DRAS), whether or not it was content, **and** data that was not content as defined under the pen register statute. Bates judged (see page 30 and following) that Congress intended to authorize DRAS collection only if it was not content. Since the Internet uses nested addressing, and subordinate addresses would be treated as content to the higher level routing entities, the government was effectively collecting metadata that was content (again, see Julian Sanchez’ explanation of why this is significant from a legal standpoint).

But here we are, just 3 years after Bates described all this in a court ruling (and 2 years after he repeated some of the same analysis in another court ruling), and the government is making the argument that metadata collected using the same method as content is not content because it doesn’t meet the “content” definition of the statute that doesn’t allow you to collect content, even while it does meet the “content” definition of the statute that allows you to collect content.

Oh, and by the way, the collection of US person Internet metadata-that-is-also-content still goes on overseas; the government’s assertion that that collection doesn’t go on anymore makes it clear it doesn’t go on under the FISA pen register statute, without ruling out such collection under other authorities.

In December 2011 , the U.S. Government decided not to seek re-authorization of the bulk collection of Internet metadata under section 402.

Which is quite different from saying – as they have in unsworn statements – that they’ve shut

down the program entirely.

The metadata that leads to the content

Finally, Clapper and Fleisch impose silence over the relationship between this metadata and content, declaring state secrets over both the scope of the TSP (and therefore implicitly, the PSP) and 702 collection, as well as,

any other information related to demonstrating that the NSA has not otherwise engaged in the content-surveillance dragnet that the plaintiffs allege

Nowhere in their declarations is there any language akin to the language Teresa Shea, NSA Director of Signals Intelligence Directorate, used just a month ago in the Larry Klayman suit.

Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. **Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities.** Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

To be fair, both of these passages use wonderfully vague language. "Content-surveillance dragnet" is something distinct from "content dragnet," the latter of which might refer to the collection but not review of content. And "content analysis" likewise assumes the content already got collected.

So both the effort to avoid describing and the effort to describe how the metadata ties directly into selecting which already-collected content to read gloss over that "already-collected" assumption (page 16 and following of the NSA IG Report describes some of this, and makes it clear the telecoms are using the metadata to pull the content for further analysis).

The thing is, the government likely has reason to be mighty uncertain about the legal status of this (or, even more likely, mighty certain but unhappy). While it is likely that the US person content systematically read using this system does not include the plaintiffs, the reason it doesn't is because the telecoms have already collected the plaintiffs' metadata (which, in the case of their Internet data, is also legally content) and because they've briefly held their content while they scan it against selected metadata identifiers selected by analyzing all metadata identifiers, including their own.

They might win an argument that this collection was not indiscriminate, but to win it, they'd have to reveal the many places in the process where they had violated wiretap laws.

Thus, Clapper is instead using Bush and Obama's favorite strategy of declaring evidence of crime a state secret. All the while boasting of his own transparency in declassifying one more tiny chunk of Bush's illegal program.

CONNING THE RECORD, CONNING THE COURTS, DEFRAUDING THE PEOPLE

In the parlance of the once and forever MTV set, civil libertarians just had one of the “Best Weeks Ever”. Here is the ACLU’s Catherine Crump weighing in on the surprising results of President Obama’s Review Board:

Friday, the president’s expressed willingness to consider ending the NSA’s collection of phone records, saying, “The question we’re going to have to ask is, can we accomplish the same goals that this program is intended to accomplish in ways that give the public more confidence that in fact the NSA is doing what it’s supposed to be doing?”

With this comment and the panel’s report coming on the heels of Monday’s remarkable federal court ruling that the bulk collection of telephone records is likely unconstitutional, this has been the best week in a long time for Americans’ privacy rights.

That “federal court ruling” is, of course, that of Judge Richard Leon handed down a mere five days ago on Monday. Catherine is right, it has been a hell of a good week.

But lest we grow too enamored of our still vaporous success, keep in mind Judge Leon’s decision, as right on the merits as it may be, and is, is still a rather adventurous and activist decision for a District level judge, and will almost certainly be pared back to some extent on appeal, even if some substantive parts of it are upheld. We shall see.

But the other cold water thrown came from Obama

himself when he gave a slippery and disingenuous press conference Friday. Here is the New York Times this morning capturing spot on the worthless lip service Barack Obama gave surveillance reform yesterday:

By the time President Obama gave his news conference on Friday, there was really only one course to take on surveillance policy from an ethical, moral, constitutional and even political point of view. And that was to embrace the recommendations of his handpicked panel on government spying – and bills pending in Congress – to end the obvious excesses. He could have started by suspending the constitutionally questionable (and evidently pointless) collection of data on every phone call and email that Americans make.

He did not do any of that.

...

He kept returning to the idea that he might be willing to do more, but only to reassure the public “in light of the disclosures that have taken place.”

In other words, he never intended to make the changes that his panel, many lawmakers and others, including this page, have advocated to correct the flaws in the government’s surveillance policy had they not been revealed by Edward Snowden’s leaks.

And that is why any actions that Mr. Obama may announce next month would certainly not be adequate. Congress has to rewrite the relevant passage in the Patriot Act that George W. Bush and then Mr. Obama claimed – in secret – as the justification for the data vacuuming.

Precisely. The NYT comes out and calls the dog a dog. If you read between the lines of this Ken Dilanian report at the LA Times, you get the

same preview of the nothingburger President Obama is cooking up over the holidays. As Ken more directly said in his tweet, "Obama poised to reject panel proposals on 702 and national security letters." Yes, indeed, count on it.

Which brings us to that which begets the title of this post: I Con The Record has made a Saturday before Christmas news dump. And a rather significant one to boot. Apparently because they were too cowardly to even do it in a Friday news dump. Which is par for the course of the Obama Administration, James Clapper and the American Intel Shop. Their raison de'être appears to be keep America uninformed, terrorized and supplicant to their power grabs. Only a big time operator like Big Bad Terror Voodoo Daddy Clapper can keep us chilluns safe!

So, the dump today is HERE in all its glory. From the PR portion of the "I Con" Tumblr post, they start off with Bush/Cheney Administration starting the "bulk" dragnet on October 4, 2001. Bet that is when it first was formalized, but the actual genesis was oh, maybe, September 12 or so. Remember, there were security daddies agitating for this long before September 11th.

Then the handcrafted Intel spin goes on to say this:

Over time, the presidentially-authorized activities transitioned to the authority of the Foreign Intelligence Surveillance Act ("FISA"). The collection of communications content pursuant to presidential authorization ended in January 2007 when the U.S. Government transitioned the TSP to the authority of the FISA and under the orders of the Foreign Intelligence Surveillance Court ("FISC"). In August 2007, Congress enacted the Protect America Act ("PAA") as a temporary measure. The PAA, which expired in February 2008, was replaced by the FISA Amendments Act of 2008, which was enacted in July 2008 and remains in effect. Today, content

collection is conducted pursuant to section 702 of FISA. The metadata activities also were transitioned to orders of the FISC. The bulk collection of telephony metadata transitioned to the authority of the FISA in May 2006 and is collected pursuant to section 501 of FISA. The bulk collection of Internet metadata was transitioned to the authority of the FISA in July 2004 and was collected pursuant to section 402 of FISA. In December 2011, the U.S. Government decided to not seek reauthorization of the bulk collection of Internet metadata.

After President Bush acknowledged the TSP in December 2005, two still-pending suits were filed in the Northern District of California against the United States and U.S. Government officials challenging alleged NSA activities authorized by President Bush after 9/11. In response the U.S. Government, through classified and unclassified declarations by the DNI and NSA, asserted the state secrets privilege and the DNI's authority under the National Security Act to protect intelligence sources and methods. Following the unauthorized and unlawful release of classified information about the Section 215 and Section 702 programs in June 2013, the Court directed the U.S. Government to explain the impact of declassification decisions since June 2013 on the national security issues in the case, as reflected in the U.S. Government's state secrets privilege assertion. The Court also ordered the U.S. Government to review for declassification all prior classified state secrets privilege and sources and methods declarations in the litigation, and to file redacted, unclassified versions of those documents with the Court.

This is merely an antiseptic version of the timeline of lies that has been relentlessly exposed by Marcy Wheeler right here on this blog, among other places. What is not included in the antiseptic, sandpapered spin is that the program was untethered from law completely and then “transitioned” to FISC after being exposed as such.

Oh, and lest anybody think this sudden disclosure today is out of the goodness of Clapper and Obama’s hearts, it is not. As Trevor Timm of EFF notes, most all of the “I Con” releases have been made only after being forced to by relevant FOIA and other court victories and that this one in particular is mostly germinated by EFF’s court order (and Vaughn index) obtained.

So, with that, behold the “I Con” release of ten different declarations previously filed and extant under seal in the *Jewel* and *Shubert* cases. Much of the language in all is similar template affidavit language, which you expect from such filings if you have ever dealt with them. As for individual dissection, I will leave that for later and for discussion by all in comments.

The one common theme that I can discern from a scan of a couple of notes is that there is no reason in the world minimally redacted versions such as these could not have been made public from the outset. No reason save for the conclusion that to do so would have been embarrassing to the Article II Executive Branch and would have lent credence to American citizens properly trying to exercise and protect their rights in the face of a lawless and constitutionally infirm assault by their own government. The declarations by Mike McConnell, James Clapper, Keith Alexander, Dennis Blair, Frances Fleisch and Deborah Bonanni display a level of too cute by a half duplicity that ought be grounds for sanctions.

The record has been conned. Our federal courts have been conned. All as the Snowden disclosures

have proven. And the American people have been defrauded by pompous terror mongers who value their own and institutional power over truth and honesty to those they serve. Clapper, Alexander and Obama have the temerity to call Ed Snowden a traitor? Please, look in the mirror boys.

Lastly, and again as Trevor Timm pointed out above, these are just the declarations for cases the EFF and others are still pursuing. What of the false secret declarations made in *al-Haramain v. Obama*, which the government long ago admitted were bogus? Why won't the cons behind "I Con" release those declarations? What about the frauds perpetrated in *Mohamed v. Jeppesen* that have fraudulently ingrained states secrets cons into the government arsenal?

If the government wants to come clean, here is the opportunity. Frauds have been perpetrated on our courts, in our name. We should hear about that. Unless, of course, Obama and the "I Cons" are really nothing more than simple good old fashioned cons.

[By the way, Christmas is a giving season. If you have extra cheer to spread, our friends like Cindy Cohn, Trevor Timm, Hanni Fakhoury and Kurt Opsahl et al at EFF, and Ben Wizner, Alex Abdo, Catherine Crump et al at the ACLU all do remarkable work. Share your tax deductible love with them this season if you can. They make us all better off.]

THE NSA REVIEW GROUP GANDERS AT METADATA

As you've no doubt heard, the NSA Review Group recommends real limits on the government's access to metadata, preferring that it be left with the telecoms and only be retained 2 years, and also recommending a higher standard for

accessing it.

Which is why I find this recommendation, to more closely watch high level security classification holders, so ironic.

The routine PCMP review would draw in data on an ongoing basis from commercially available data sources, such as on finances, court proceedings, and driving activity of the sort that is now available to credit scoring and auto insurance companies. Government-provided information might also be added to the data base, such as publicly available information about arrests and data about foreign travel now collected by Customs and Border Patrol.

Those with extremely high Access Scores might be asked to grant permission to the government for their review by a more intrusive Additional Monitoring Program, including random observation of the meta-data related to their personal, home telephone calls, e-mails, use of online social media, and web surfing. Auditing and verification of their Financial Disclosure Forms might also occur.

A data analytics program would be used to sift through the information provided by the Additional Monitoring Program on an ongoing basis to determine if there are correlations that indicate the advisability of some additional review.

It rationalizes this intrusiveness by pointing out that clearance jobs are privileges, not a right.

We recognize that such a program could be seen by some as an infringement on the privacy of federal employees and contractors who choose on a voluntary basis to work with highly sensitive information in order to defend our

nation. But, employment in government jobs with access to special intelligence or special classified programs is not a right. Permission to occupy positions of great trust and responsibility is already granted with conditions, including degrees of loss of privacy.

And, apparently unlike the phone and Internet dragnet, it proposes to start with a pilot.

But I wonder if this metadata program would have the same problem the NSA's dragnets do: they haven't ever proven they work as planned.

NSA'S BID FOR A 6 MONTH DELAY IN PROTECTING LARRY KLAYMAN'S PHONE RECORDS

The White House has announced they're going to release the recommendations of the Committee to Make You Love the Dragnet today. Given that the report recommends putting the dragnet into someone else's hands, I suspect the White House changed plans (It was going to release the report in mid-January) as a way to stave off the Klayman and other suits.

Given that we expect that recommendation – and that the government claims it'd take years to effect – I want to point to a claim that NSA Director of Signals Intelligence Division Theresa Shea made in her declaration in the Klayman suit. She claimed it would be an onerous process to take Larry Klayman's call records out of the dragnet.

Beyond harming national security and the Government's counterterrorism capabilities, plaintiffs' proposed preliminary injunction would seriously burden the Government. While plaintiffs seek an order barring the Government from collecting metadata reflecting their calls, the Government does not know plaintiffs' phone numbers, and would need plaintiffs to identify all numbers they use to even attempt to implement such an injunction. Ironically, as explained above, these numbers are not currently visible to NSA intelligence analysts unless they are within a three hops of a call chain of a number that based on RAS is associated with a foreign terrorist organization.

Even if plaintiffs' phone numbers were available, extraordinarily burdensome technical and logistical hurdles to compliance with a preliminary injunction order would remain. Technical experts would have to develop a solution such as removing the numbers from the system upon receipt of each batch of metadata or developing a capability whereby plaintiffs' numbers would be received by NSA but would not be visible in response to an authorized query. To identify, design, build, and test the best implementation solution would potentially require the creation of new full-time positions and could take six months or more to implement. Once implemented, any potential solution could undermine the results of any authorized query of a phone number that based on RAS is associated with one of the identified foreign terrorist organizations by eliminating, or cutting off potential call chains. If this Court were to grant a preliminary injunction and the defendants were to later prevail on the merits of this litigation, it could prove extremely difficult to

develop a solution to reinsert any quarantined records and would likely take considerable resources and several months to build, test, and implement a reinsertion capability suited to this task.

Judge Richard Leon treated this complaint as the obvious bullpuckey it clearly is.

[T]he Government says that it will be burdensome to comply with any order that requires the NSA to remove plaintiffs from its database. Of course, the public has no interest in saving the Government from the budens of complying with the Constitution! Then, the Government frets such an order “could ultimately have a degrading effect on the utility of the program if an injunction in this case precipitated successful requests for such relief by other litigants.” For reasons already explained, I am not convinced at this point in the litigation that the NSA’s database has ever truly served the purpose of rapidly identifying terrorists in time-sensitive investigations, and so I am *certainly* not convinced that the removal of two individuals from the database will “degrade” the program in any meaningful sense.⁶⁸

[snip]

In [staying my order to destroy the plaintiffs’ metadata] I hereby give the Government fair notice that should my ruling be upheld, this order will go into effect forthwith. Accordingly, I fully expect that during the appellate process, which will consume at least the next six months, the Government will take whatever steps necessary to prepare itself to comply with this order when, and if, it is upheld. Suffice it to say, requesting further time to comply with

this order months from now will not be well received and could result in collateral sanctions.

68 To the extent that removing plaintiffs from the database would create the risk of “eliminating, or cutting off potential call chains,” the Government concedes that the odds of this happening are miniscule. (“[O]nly a tiny fraction of the collected metadata is ever reviewed”) (“Only the tiny fraction of the telephony metadata records that are responsive to queries authorized under the RAS standard are extracted, reviewed, or disseminated. . . .”). [citations removed]

But the plea for time— when it’s crystal clear NSA could start treating Larry Klayman’s data like a high volume number they intentionally defeat on intake tomorrow — made me wonder what purpose this complaint was really meant to serve, especially given James Cole’s refusal the other day to answer whether the Leahy-Sensenbrenner bill would eliminate bulk collection, which Jennifer Granick likens to a coup.

Responding to a question at yesterday’s hearing on the bill, Cole said, “Right now the interpretation of the word ‘relevant’ is a broad interpretation. Adding ‘pertinent to a foreign agent’ or ‘somebody in contact with a foreign agent’ could be another way of talking about relevance as it is right now. We’d have to see how broadly the court interprets that or how narrowly.” In other words, the FISA court might let us keep doing what we’re doing no matter what the law says and despite Congress’ intent.

All courts issue opinions about what the laws that legislatures pass mean. These opinions are called the “common law”.

But common law interpretations of statutes are only legitimate if they are fair and reasonable interpretations.

The NSA has a great track record getting FISC judges to interpret even obviously narrow phrases in surprisingly broad ways.

[snip]

Time and again, the FISC accepts the Administration's shockingly flimsy arguments. As a set, the few public FISC opinions we've seen suggest that the Executive Branch—in cahoots with a few selected judges—has replaced legitimate public statutes with secret, illegitimate common law.

The rule of law is a basic democratic principle meaning that all members of a society—individuals, organizations, and government officials—must obey publicly disclosed legal codes and processes. If Cole is right that, try as it might, Congress cannot end bulk collection because the secret FISA court may defer to the NSA's interpretation of the rules, there is no rule of law. The NSA is in charge, the FISA court process is just a fig leaf, and this is no longer a democracy. There's been a *coup d'etat*.

But it appears that not even the FISC judges are always in on the game. After all, at the moment when Judges Walton and Bates started reining in the Internet dragnet in the US, NSA started rolling out an expanded Internet dragnet program – which made it easier to pick up US person data and presumably easier to disseminate it – overseas. With that 6 month delay, would NSA just be figuring out how to maintain the dragnet function, but beyond the reach of meddling judges like Richard Leon?

The NSA suggested it would need 6 months notice to take just two people out of the dragnet. I

can imagine no feasible technical reason that's true.

So why were they implying they'd need that 6 months?

THE PURPOSE(S) OF THE DRAGNET, REVISITED

As I noted the other day, one basis Judge Richard Leon used to find that the dragnet was likely unconstitutional was that it wasn't all that useful. But I was particularly interested in the evidence he points to to establish that (see page 61 of his ruling), because it and the underlying basis for it reveal far more about how the government uses the dragnet than we've seen.

Leon points to the three cases in which the phone dragnet was supposed to be useful, which he gets from the declaration of FBI Acting Assistant Director Robert Holley. Holley claims the dragnet was useful in the Khalid Ouazzani, David Headley, and Najibullah Zazi cases (though Holley does not mention Ouazzani by name), using the following language.

In January 2009, using authorized collection under Section 702 of the Foreign Intelligence Surveillance Act to monitor the communications of an extremist overseas with ties to al-Qa'ida, NSA discovered a connection with an individual based in Kansas City. NSA tipped the information to the FBI, which during the course of its investigation discovered that there had been a plot in its early stages to attack the New York Stock Exchange. After further investigation, NSA queried the telephony metadata to ensure that all potential

connections were identified, which assisted the FBI in running down leads.

[snip]

At the time of his arrest, Headley and his colleagues, at the behest of al-Qa'ida, were plotting to attack the Danish newspaper that published cartoons depicting the Prophet Mohammed. Headley was later charged with support for terrorism based on his involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Collection against foreign terrorists and telephony metadata analysis were utilized in tandem with FBI law enforcement authorities to establish Headley's foreign ties and them in context with his U.S. based planning efforts.

[snip]

NSA received Zazi's telephone number from the FBI and ran it against the Section 215 telephony metadata, identifying and passing additional leads back to the FBI for investigation. One of these leads revealed a previously unknown number for co-conspirator Adis Medunjanin and corroborated his connection to Zazi as well as to other U.S.-based extremists.

First, note what's missing? Any mention of Basaaly Moalin, the **only** defendant for which the government claims the phone dragnet was critical to his identification. Holley may have left Moalin out because of the timing: DOJ submitted his declaration on November 12, the day before the hearing on Moalin's bid for a new trial and two days before Jeffrey Miller's ruling rejecting that. Did DOJ think they might lose that argument, and so left it out out of fear it would make them more likely to lose this one (Leon does acknowledge Miller's ruling in his own). Or was the case just so dated they

chose not to mention it?

Whatever the reason, they're left describing three cases in which even Keith Alexander admits the dragnet was at best only helpful.

But note the other thing: Up until now, the government has only described how the dragnet was useful in the Zazi case. While in its propaganda about 54 plots or maybe just terrorist events thwarted, it has implicitly suggested that only those with a US-nexus could involve the dragnet, I know of no other instance where they made it clear that they sort of used it in the Headley and Ouazzani cases (I'm going to check the declarations in the parallel suits later).

In both cases, it appears, the government only used it after the fact (which is how they used it in the Boston Marathon attack, which bizarrely also goes unmentioned).

They found the claimed NYSE plot (which wasn't really a plot), and only later consulted the dragnet. They arrested Headley (DEA's informant, remember), and then used the dragnet to put this US informant's foreign ties in context.

That at least suggests the possibility that, as the challenge of getting the dragnet reauthorized in 2009, FBI started having its Agents consult the dragnet in any case involving Section 702.

Note one more thing about the language Holley uses: while he describes the telephony metadata consulted in the Zazi case Section 215 data, he calls the others simply telephony metadata. Given what we now know about the way that all metadata collections are accessible from the same interface and NSA analysts are encouraged to use E0 12333 collections when they'll return the same results as a Section 215 query, this raises the distinct possibility that the Ouazzani and Headley queries weren't even technically Section 215 queries. (There are vague hints in other documents that the NSA's

“data integrity analysts” may remove informants from the dragnet – which they might do to keep FBI and other federal Agents out of the dragnet – which I may return to later.)

Which means it’s not only possible they’re doing queries after the fact to be able to say they used the dragnet, but they’re technically doing queries of a different dragnet.

I find that slippery language of particular interest given the advantages Holley says the dragnet offers. First, he says the dragnet offers advantages over other possible means of chaining.

The NSA bulk collection program at issue here presents distinct advantages. The contact chaining capabilities offered by the program exceed the chaining that is performed on data collected pursuant to other means, including traditional means of case-by case intelligence gathering targeted at individual telephone numbers such as subpoena, warrant, national security letter, pen-register and trap-and-trace (PR/TT) devices, or more narrowly defined orders under Section 215.

He lays out what may be just some of the other possibilities (I find it of particular interest that he includes “more narrowly defined orders under Section 215,” which suggests they may replicate Section 215 collection for non-counterterrorism uses). But his list doesn’t necessarily exclude E0 12333 collected dragnet (which would be broader because it included foreign to foreign contacts, but more narrow because it would not be comprehensive for US contacts).

Holley then points to the the “agility” with which NSA can do second-order chaining (again raising questions why they didn’t include Moalin, who was found on a second hop) and the ability to identify chains across multiple

providers

This is so in at least two important respects, namely, the NSA's querying and analysis of the aggregated bulk telephony metadata under this program. First, the agility of querying the metadata collected by NSA under this program allows for more immediate contact chaining, which is significant in time-sensitive situations of suspects' communications with known or as-yet unknown co-conspirators. For example, if investigators find a new telephone number when an agent of one of the identified international terrorist organizations is captured, and the Government issues a national security letter for the call details for that particular number, it would only be able to obtain the first tier of telephone number and contacts and, in rare instances, if the second tier of contacts if the FBI separately demonstrates the relevance of the second-generation information to the national security investigation. At least with respect to the vast majority of national security letters issued, new national security letters would have to be issued for telephone numbers identified in the first tier, in order to find an additional tier of contacts. The delay inherent in issuing new national security letters would necessarily mean losing valuable time.

Second, aggregating the NSA telephony metadata from different telecommunications providers enhances and expedites the ability to identify chains of communications across multiple providers. Furthermore, NSA disseminations provided to the FBI from this program may include NSA's analysis informed by its unique capabilities.

This last paragraph is particularly interesting. The reference to “NSA’s analysis informed by its unique capabilities” likely refers to stuff the NSA can do once it has deposited queries into the corporate store (all the more so given the reference in the Headley description to **“Collection against foreign terrorists and telephony metadata analysis** were utilized in tandem with FBI law enforcement authorities”), which far exceed simple chaining.

Which brings me to the declaration of Theresa Shea, the Director of NSA’s Signals Intelligence Directorate.

Her declaration is patently dishonest in parts: it doesn’t mention the use of dragnet information to identify informants (as opposed to potential terrorists); it doesn’t disclose all the violations in 2009 and pretends Congress got timely notice of violations; it doesn’t describe the ease with which NSA accesses US person content via back door access; it doesn’t admit that NSA lumps and chains phone metadata in with Internet metadata.

But her declaration does provide this description of how NSA uses the dragnet to decide which communications to prioritize.

Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. **Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities.** Such persons are of heightened interest if they are in a communication network with persons

located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

She implies this is used solely with non-US persons, but the example of Moalin, not to mention everything we know about minimization procedures, suggests they use it to read the incidentally collected content of US persons in communication with foreigners, and (in his case) then use that content to establish probable cause to get his content directly.

Now, we've known the government does this for months; both James Clapper and Edward Snowden described using the metadata to find which communications to read (and General Alexander used the same library metaphor Clapper did in last week's SJC hearing).

But this is as close as the government has come to officially admitting that the metadata does, in fact, lead directly to accessing content, that since they collect "everything" – both metadata and content – from at least selected targets, a metadata connection amounts to accessing content.

If that's right, though, it means any US persons whose contacts are deposited into the corporate store are likely to have their contents read (and we know NSA doesn't require Reasonable Articulable Suspicion to do that). The NSA and FBI together got very close to admitting that a system that needs only RAS to initiate intrusive contact chaining serves as the justification – literally "the key" – to access US person content without further RAS. Which would be a remarkably different Fourth Amendment equation than even billions of pen registers, which is what the government wants to pretend this is.

But that's not all. Holley's declaration

provides hints about some other ways this contact chaining is used. As I've been predicting for months and months, Holley suggests this data goes into things like No Fly and State and Treasury Terrorist designations – designations that are almost impossible to challenge in court.

Counter-terrorism investigations serve important purposes beyond the ambit of routine criminal inquiries and prosecution, which ordinarily focus retrospectively on specific crimes that have already occurred and the persons known or suspected to have committed them. The key purpose of terrorism investigations, in contrast, is to prevent terrorist attacks before they occur. Terrorism investigations also provide the basis for, and inform decisions concerning other measures needed to protect the national security, including: **excluding or removing persons involved in terrorism from the United States; freezing assets of organization that engage in or support terrorism;** securing targets of terrorism; providing threat information and warnings to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism threats. [my emphasis]

While Holley doesn't connect this passage directly with the dragnet, it appears in a declaration about the dragnet. Which means, rather unsurprisingly, that the government may be basing due process free infringements on certain basic privileges – like flying and banking – on the contact chaining including every single American.

Judge Leon only looked at the unconvincing explanations of how the dragnet tied to the three cases presented by the FBI to rule this

was probably unconstitutional (he also cited ProPublica's debunking of such claims). He didn't look at any of the far more ominous language in the declarations before him, which hint at – but ultimately stop short of clarity or candor – potentially far greater constitutional problems with the dragnet. Let's hope one of the other judges reviewing these suits asks for more clarity.

DIANNE FEINSTEIN GLOSSES JEFFREY MILLER PHONE DRAGNET DECISION

Dianne Feinstein just released a statement effectively saying she likes the FISA Court phone dragnet decisions and the one Judge Jeffrey Miller made in the Moalin case better than the one Richard Leon issued yesterday.

Clearly we have competing decisions from those of at least three different courts (the FISA Court, the D.C. District Court and the Southern District of California). I have found the analysis by the FISA Court, the Southern District of California and the position of the Department of Justice, based on the Supreme Court decision in Smith, to be compelling.

But I'm particularly interested in the way she describes the Miller decision.

It should be noted that last month Judge Jeffrey Miller of the Southern District of California found the NSA business records program to be constitutional.

Judge Miller was ruling on a real world terrorist case involving the February 2013 conviction of Basaaly Moalin and three others for conspiracy and providing material support to the Somali terrorist organization Al-Shabaab. In that case, the NSA provided the FBI with information gleaned from an NSA query (under Section 215) of the call records database that established a connection between a San Diego-based number and a number known to be used by a terrorist with ties to al Qaeda.

In upholding these convictions, Judge Miller cited *Smith v. Maryland* (1979) the controlling legal precedent and held the defendants had 'no legitimate expectation of privacy' over the type of telephone metadata acquired by the government—which is the 'to' and 'from' phone numbers of a call, its time, its date and its duration. There is no content, no names and no locational information acquired.

As a threshold matter, Judge Miller did not decide last month that the phone dragnet was constitutional. He decided sometime around June 5, 2012, and that decision remains sealed in its entirety. He treated Moalin's bid for a new trial as a reconsideration of his earlier decision, stating he had, "already considered and addressed many of the FISA and CIPA arguments from a federal and constitutional law perspective." He deliberated just one day after the hearing on a new trial before rejecting the motion. Which means that his decision rests primarily on whatever representations the government made in secret – and none of us have gotten to see that decision.

If Senator Feinstein would like to use her position on the Senate Intelligence and Judiciary Committees to liberate that decision given that she's relying on it, by all means let's have some transparency!

Now look at how Feinstein characterizes the issue before Miller:

[T]he NSA provided the FBI with information gleaned from an NSA query (under Section 215) of the call records database that established a connection between a San Diego-based number and a number known to be used by a terrorist with ties to al Qaeda.

That is, she characterizes Miller's review as weighing whether using an (at least) second-degree hop in a database to establish probable cause is Constitutional.

But that's most definitely not what Miller did. Instead, he ignored the database entirely (the word "database" doesn't appear in his ruling), and assessed the use of what Feinstein describes as a database query as two separate pen registers.

Defendants argue that the collection of telephony metadata violated Defendant Moalin's First and Fourth Amendment rights. **At issue are two distinct uses of telephone metadata obtained from Section 215. The first use involves telephony metadata retrieved from communications between third parties, that is, telephone calls not involving Defendants.** Clearly, Defendants have no reasonable expectation of privacy to challenge any use of telephony metadata for calls between third parties. See *Steagald v. United States*, 451 U.S. 204, 219 (1981) (Fourth Amendment rights are personal in nature); *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) ("Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted."); *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990) (the term "people" described in the Fourth Amendment are persons who are part of

the national community or may be considered as such). As noted in Steagald, “the rights [] conferred by the Fourth Amendment are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched.” 451 U.S. at 219. **As individuals other than Defendants were parties to the telephony metadata, Defendants cannot vicariously assert Fourth Amendment rights on behalf of these individuals.** To this extent, the court denies the motion for new trial.

The second use of telephony metadata involves communications between individuals in Somalia (or other countries) and Defendant Moalin. The following discusses whether Defendant Moalin, and other Defendants through him, have any reasonable expectation of privacy in telephony metadata between Moalin and third parties, including co-defendants. [my emphasis]

I believe that in documents that have been released since Miller’s ruling, the government distinguished this from pen registers (digging up those references now). But one thing’s clear: Miller didn’t approve the use of a database to show that his two-degree link between Moalin and Aden Ayro amounted to probable cause that he was an agent of a foreign power. He approved of two or more discrete pen registers.

That may or may not amount to a legal difference (Leon didn’t consider the database as such either). But I find it mighty telling that Feinstein describes the dragnet in terms her favored criminal ruling does not.

THE PRE-DRAGNET COLD WAR CONTACT CHAINING

I'm still working through some things from Judge Richard Leon's injunction against the phone dragnet.

But for the moment I wanted to point to something the government claimed in the FBI's declaration in the case, by Acting Assistant Director Robert Holley. He says,

For decades reaching back to the Cold-War era, the FBI has relied on contact chaining as a method of detecting foreign espionage networks and operatives, both in the United States and abroad, and disrupting their plans.

The language here seems somewhat forced. "Decades reaching back to the Cold War-era" might only mean 1988.

Moreover, the fact that FBI claims they've been doing this for "decades" suggests they've been doing it for decades before they put together the phone dragnet, even decades before they required telecoms to keep phone records for 18 months.

Doesn't that mean it's possible to do successfully without the dragnet and without 5 years of data?

If the technique, absent the dragnet, was effective against the Soviet Union, why do we need a dragnet against a less powerful adversary now?

RICHARD LEON: A PHONE DRAGNET IS NOT A SPECIAL NEED

As I noted briefly in this post, Judge Richard Leon ruled that Judicial Watch's Larry Klayman is very likely to succeed in his suit challenging the phone dragnet on Constitutional grounds. He issued an injunction requiring NSA to take out Klayman's data, but stayed that decision pending appeal.

While many civil liberties lawyers are hailing the decision, the its strength might be measured by the fact that Mark Udall and Jim Sensenbrenner both used it as a call to pass Leahy-Sensenbrenner; they did not celebrate the demise of the dragnet itself. That is, it is almost certain that this decision will not, by itself, end the dragnet.

I suspect this ruling will serve to break the ice for other judges (there are several other suits, a number of them launched by entities – like the ACLU – that I expect to have better command of the details of the dragnet and the reasons it is unconstitutional, which may lead to a stronger opinion). And to the extent it stands (don't hold your breath) it will begin to chip away at NSA's claims that searches don't happen on collection, but on database access.

And on one point, I think Leon's ruling provides a really important baseline on the matter of special needs.

As Orin Kerr sketches out roughly here (and I agree with much of what he says about Leon's ruling), Leon basically held that *Smith v. Maryland* didn't apply in the era of smart phones. From there, he moved onto Fourth Amendment analysis, which involves an analysis of whether the special need of hunting terrorists merits the huge privacy infringement of collecting all phone records in the US. After reviewing the precedents on special needs, Leon

writes,

To my knowledge, however, no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. In effect, the Government urges me to be the first non-FISC judge to sanction such a dragnet.

Then Leon goes on to challenge the government's claims about the need involved.

The Government asserts that the Bulk Telephony Metadata Program serves the "programmatic purpose" of "identifying unknown terrorist operatives and preventing terrorist attacks."

[snip]

A closer examination of the record, however, reveals the Government's interest is a bit more nuanced—it is not merely to investigate potential terrorists, but rather, to do so *faster* than other investigative methods might allow.

Which brings him to the same issue Ron Wyden and Mark Udall keep pointing to: the NSA simply doesn't have evidence of this actually having worked.

Yet, turning to the efficacy prong, the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and

protecting against terrorist attack”
involved any urgency.

Now, I actually think the NSA and FBI declarants in this case begin to hint at the real purpose of the dragnet – I’ll come back to that once PACER recovers from what everyone jokes is NSA retaliation for this ruling.

But with regards to accomplishing the purpose the NSA claims the dragnet serves, there’s no evidence to show. Leon finds that absent real proof that the dragnet works, Klayman’s privacy interests outweigh the Government’s need.

Given the limited record before me at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.

[snip]

Thus, plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government’s interest in collecting and analyzing build telephony metadata and therefore the NSA’s bulk collection program is indeed an unreasonable search under the Fourth Amendment.

Now, to be clear, before Leon gets here, he has to get by *Smith v. Maryland*, and I agree with Kerr that his argument there isn’t all that strong (though I disagree with Kerr that it couldn’t be).

But one big takeaway from this ruling –whether the DC Circuit overturns it or not – is that it

will be very hard for the government to make the case that the need the dragnet serves outweighs the privacy cost.

Probably not with this ruling, but it may not be long before the government has to face up to the fact that its dragnet really hasn't shown any results.

Update: New Yorker's Amy Davidson writes, "But what his ruling does is deprive the N.S.A. of the argument of obviousness: the idea that what it is doing is plainly legal, plainly necessary, and nothing for decent people to worry about." That's about what I mean by Leon breaking the ice.

THAT PIRATE MAY BE THE MISSING LINK WE SHOULD DRONE KILL

As I mocked last night, 60 Minutes decided to use pirate data collected under E0 12333 to demonstrate how it conducts call chaining on US citizen data collected under Section 215. But the exchange is rather interesting for the way the NSA analyst, Stephen Benitez, describes finding a potentially key player in a network of pirates.

Metadata has become one of the most important tools in the NSA's arsenal. Metadata is the digital information on the number dialed, the time and date, and the frequency of the calls. We wanted to see how metadata was used at the NSA. 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.** [my emphasis]

Compare the language Benitez uses here with that which Gregory McNeal used to describe drone targeting back in February.

Networked based analysis looks at terrorist groups as nodes connected by links, and assesses how components of that terrorist network operate together and independently of one another. **Those nodes and links, once identified will be targeted with the goal of disrupting and degrading their functionality.** To effectively pursue a network based approach, bureaucrats rely in part on what is known as "pattern of life analysis" which involves connecting the relationships between places and people by tracking their patterns of life. This

analysis draws on the interrelationships among groups “to determine the degree and points of their interdependence.” It assesses how activities are linked and looks to “determine the most effective way to influence or affect the enemy system.”

[snip]

Viewing targeting in this way demonstrates how **seemingly low level individuals such as couriers and other “middle-men” in decentralized networks such as al Qaeda are oftentimes critical to the successful functioning of the enemy organization. Targeting these individuals can “destabilize clandestine networks by compromising large sections of the organization, distancing operatives from direct guidance, and impeding organizational communication and function.”** Moreover, because clandestine networks rely on social relationships to manage the trade-off between maintaining secrecy and security, attacking key nodes can have a detrimental impact on the enemy’s ability to conduct their operations. [my emphasis]

That is, the language describing the process behind signature strikes closely matches the language describing NSA’s targeting for wiretapping. Both these analyses are doing the same thing: trying to find the key nodes in networks of people (though the drone targeting appears to draw in additional intelligence about someone’s observed actions and locations).

Now, as I said, when Benitez used the word “target,” he was presumably discussing only targeting for surveillance, not for drone killing (besides, thus far we haven’t drone killed any pirates I know of).

But it is very easy to see what kind of role

metadata analysis would play in the early stages of targeting a signature strike, because that's precisely how the intelligence community identify the nodes that, McNeal tells us, they're often targeting when they conduct signature strikes. Wiretap the person at that node and you may learn a lot (that's also probably the same kind of targeting they do to select potential informants, as we know they do with metadata), kill that person and you may damage the operational capabilities of a terrorist (or pirate) organization.

When the WaPo reported on NSA's role in drone killing, it focused on how NSA collected content associated with a known target – Hassan Ghul – to pinpoint his location for drone targeting.

But NSA probably plays a role in the far more controversial targeting of people we don't know for death, with precisely the kind of contact chaining it uses on US persons.

Note, in related news, Richard Leon has just ruled for Larry Klayman in one of the first suits challenging the phone dragnet (with the injunction stayed pending appeal). I'll have analysis on that later.