

THE GOVERNMENT PLAYS CONNECT-THE- DOTS DIFFERENTLY THAN THEY SAY

In my continuing obsession to understand precisely how the government really uses the dragnet, consider this post, in which NSA Review Group member Geoffrey Stone conducts (IMO) inadequate analysis to conclude the phone dragnet is probably unconstitutional.

In it, he provides this description of how the government uses the phone dragnet:

In 2012, the NSA queried a total of 288 phone numbers. Based on these queries, the NSA found 16 instances **in which a suspect phone number was directly or indirectly in touch with another phone number that the NSA independently suspected of being associated with terrorist activity**. In such cases, the NSA turns the information over to the FBI for further investigation.

In terms of the “connect the dots” metaphor, the purpose of the program is not so much to discover new “dots” but to determine if there are connections between two or more already suspect “dots.” **For example, if a phone number belonging to a terrorist suspect in Pakistan is found to have called a phone number in the United States that the government independently suspects belongs to a person involved in possible terrorist activity**, alarm bells (figuratively) go off very loudly, alerting the government to the need for immediate attention. [my emphasis]

I don’t think this can be an accurate description of how the dragnet works.

It is close to what happened with Adis Medunjanin. As the FBI was honing in on Najibullah Zazi, the NSA did a query and found a new cell phone for Medunjanin, though they already knew Medunjanin was a likely accomplice of Zazi's through via travel records. The government says they were particularly interested in this phone because it was in contact with other extremists. Thus, they found a brand new phone number, but one that ended up being associated with both a suspect (Medunjanin) and other suspects (the other people that phone was in contact with).

But that cell phone for Medunajnin was a brand new number to the NSA, at least according to their reports.

The claim may still be true if they used burner matching to identify Medunjanin as a match to the other phone record they had on him. But it seems this process would have to involve additional information about Medunjanin at some point – at the very least, the match of those travel documents to that phone number, if not his identity.

In other words, this only seems to make sense if they had Medunjanin's "identity" in some form or another, belying their claims not to have identities while they're contact chaining.

The description is potentially more problematic with Basaaly Moalin. In his case, the stated explanation for what happened is they found his number on a second-degree search, sent it to the FBI, and the FBI learned he was the guy who had previously been investigated in 2003.

The problem might be alleviated in two ways: first, if the *hawala* through which Moalin was sending money to Ayro, was also tied to a suspect number. That's a distinct possibility: but the question is, how does that identity as a suspect number get communicated to NSA? If NSA already had it, doesn't it mean they've got more suspect numbers sitting somewhere than have been RAS approved?

The other possibility is that Moalin himself was still identified as a suspect number from the investigation back in 2003 – that an investigation that turned up no evidence might still, during the era of the illegal program, have gotten someone nominated as a suspect number under Cheney's program, and they never purged the system entirely (which would seem to be supported by the 2009 problems, which showed they hadn't turned off the illegal program features).

Either of these possibilities, of course, would raise new concerns about the NSA program.

But the description would also raise real issues, both about the honesty of witnesses and the potential efficacy of the system. If the NSA only triggers on people who've got ties to a second suspect number (which is entirely different than what they've been saying) then it could not possibly alert the government to a fully compartmented lone actor (someone like, say, Faisal Shahzad). That is, it would only find people who were engaged in the kind of elaborate planning seen before the government dismantled al Qaeda, but would not find the kind of individual extremists we've seen almost exclusively (with the exception of Zazi) for years.

This would answer the question of whether the NSA is finding the right numbers, in that it would be less likely to find someone innocent. It also might explain why the program didn't find Shahzad. But it would also mean it does (as presented) far less than the NSA has been saying it does.

I don't actually believe that, but that is what it would suggest.

ROBERT LITT AND MIKE ROGERS KNOW CONGRESS HASN'T RATIFIED THE PHONE DRAGNET

WaPo has a biting profile of Robert Litt, ODNI's General Counsel who made one more failed attempt to rationalize James Clapper's lies to Congress last week.

One of the most newsworthy bits is that WaPo published the name of Alfreda Frances Bikowsky, the analyst who got Khaled el-Masri kidnapped and tortured by mistake, for the first time.

A far more subtle but equally important detail comes in its description of why House Intelligence Chair Mike Rogers banned Litt from appearing before the Committee last summer.

Some lawmakers have found Litt's manner off-putting at best. Rogers, the chairman of the House Intelligence Committee, made clear to the DNI's office last summer that Litt was no longer welcome before his panel.

"The committee has not found Bob to be the most effective witness to explain complex legal and policy issues," said a U.S. government official familiar with the falling-out. Rogers was also bothered that **Litt faulted the committee for not doing more to share information about the surveillance programs with other members, unaware that doing so would have violated committee rules.** [my emphasis]

For what it's worth, I suspect Rogers is not worried as much about Litt's honesty (Rogers hasn't objected to James Clapper or Keith

Alexander's lies, for example, and has himself been a key participant in sustaining them), but rather, for his usual candor and abrasiveness, which the article also shows inspiring members of Congress to want to repeal the dragnet. Litt couches his answers in legalese, but unlike most IC witnesses, you can often parse it to discern where the outlines of truth are.

But I am acutely interested that Litt blames Rogers for not "doing more to share information about the surveillance programs with other members."

That refers, of course, to Rogers' failure to make the Administration's notice on the phone dragnet available to members in 2011, before the PATRIOT Reauthorization. As a result of that, 65 Congressmen voted to reauthorize the PATRIOT Act without full notice (perhaps any formal notice) of the phone dragnet – a sufficiently large block to make the difference in the vote. In spite of that fact, the Administration and even FISA Judges have repeatedly pointed to Congress' reauthorization of the phone dragnet to explain why it's legal even though it so obviously exceeds the intent of the Section 215 as passed.

Apparently Litt blames Rogers for that. And doing so got him banished from the Committee.

Frankly, Litt is right in this dispute. Rogers' excuse that committee rules prevented him from sharing the letter the Administration stated they wanted to be shared with the rest of Congress rings hollow, given that just one year earlier, Silvestre Reyes **did** make the previous letter available. If committee rules prevent such a thing, they are Rogers' committee rules, and they were fairly new at the time.

(Ironically, by imposing those rules, Rogers prevented members of his own party, elected with strong Tea Party backing, from learning about intelligence programs, though he may have just imposed the rules to increase the value of his own special access.)

So it is Rogers' fault the Administration should

not be able to claim Congress ratified the FISA Court's expansive understanding of Section 215.

And Rogers and Litt's spat about it make it clear they both know the significance of it: claims of legislative ratification fail because Congress did not, in fact, know what they were voting on, at least in 2011.

Unsurprisingly, that has not prevented the Administration from making that claim. Litt himself made a variety of it before PCLOB in November, months after he had this fight with Rogers.

[NSA General Counsel Raj] DE: So in other words, and some of this is obviously known to you all but just to make sure members of the public are aware, not only was this program approved by the Foreign Intelligence Surveillance Court every 90 days, it was twice, the particular provision was twice re-authorized by Congress with full information from the Executive Branch about the use of the provision.

[snip]

MR. LITT: I just want to add one very brief comment to Raj's in terms of the extent to which Congress was kept informed. By statute we're required to provide copies of significant opinion and decisions of the FISC to the Intelligence and Judiciary Committees of both Houses of Congress and they got the materials relating to this program, as we were required to by law.

Now, Litt's interjection here is particularly interesting. He doesn't correct De. He shifts the claim somewhat, to rely on Judiciary and Intelligence Committee notice. But even there, his claim fails, given that the Administration did not provide all relevant opinions to those Committees until after the first dragnet reauthorization in 2010. Litt probably thinks

that's okay because he didn't qualify **when** Congress got the materials.

But it's still a blatant lie, according to the public record.

More significantly, the Administration repeated that lie to both the FISC and, more significantly still, the 3 Article III Judges presiding over challenges to the dragnet generally.

The Administration keeps running around, telling everyone who is obligated to listen that Congress has ratified their expansive interpretation of the phone dragnet. It's not true. And the fact that Litt and Rogers fought – way back in the summer – over who is responsible makes it clear they know it's not true.

But they still keep saying it.

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 E0 12333 collected data, these targets do not have to have been reviewed for Reasonable Articulate 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 E0 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 of 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.

RICHARD CLARKE ALLUDES TO THE REAL COSTS OF THE DRAGNET

New America Foundation did a study of 225 terrorist plots to try to discern the source of the investigation. There are numerous obvious flaws to the study – many of which stem from the

government's own efforts to obscure the sources of what they do, some of which stem from a lack of awareness about how the government responded to other tips by collecting more NSA intelligence, some of which stem from ignoring the dragnet that existed in illegal form before the FISC-approved one.

With those caveats, NAF finds what has been reported for months: only the Basaaly Moalin's provision of less than \$10,000 to al-Shabaab stemmed from the phone dragnet.

Which provides the WaPo with another opportunity to report this as news. I'll take it: any little bit helps!

WaPo and NAF also report what I reported 5 months ago: that the government delayed 2 months after identifying Moalin's ties indirectly to Aden Ayro before wiretapping him. Remember, they say they need the dragnet to avoid delays in investigation.

Perhaps the most interesting part of WaPo's report on this, though, are Richard Clarke's comments. As a follow-up on the NSA Review Group's comment on the risk to quality of life posed by the dragnet, Clarke claims the dragnet would still be too intrusive if it had contributed to every plot.

"Although we might be safer if the government had ready access to a massive storehouse of information about every detail of our lives, the impact of such a program on the quality of life and on individual freedom would simply be too great," the group's report said.

Said Clarke: "Even if NSA had solved every one of the [terrorist] cases based on" the phone collection, "we would still have proposed the changes."

This is actually a fairly stunning comment (and not one, I suspect, Mike Morell, who is also quoted, would support). Even if the dragnet had

identified every potential terrorist plot, Clarke says, it would still be too intrusive.

I think the dragnet is plenty intrusive – and I think plenty of the ways it infringes on privacy are those not accounted in NAF’s analysis (such as the use of the dragnet to pick targets for informants or conduct back door searches). Still: to suggest the dragnet would not be worth every single one of these leads?

WHEN FBI DIRECTOR JIM COMEY ATE 20 JOURNALISTS FOR LUNCH, NSL EDITION

Yesterday, charismatic FBI Director Jim Comey had what was alternately described as a “lunchtime interview” and a “roundtable” with a bunch of journalists. (See NYT, ABC, AFP, NPR, McClatchy, HuffPo, LAT, WSJ, Politico, AP)

Where he proceeded to eat them for lunch.

While he addressed many topics, it appears one of his key goals was to lobby to keep National Security Letter authority as is rather than adopt the NSA Review Group’s recommended changes.

Here’s how Politico described it (I don’t mean to pick on Josh Gerstein; his was one of the most thorough reports of what Comey said, even in spite of writing one of the single bylined stories; the outlets above all published some version of this story.)

“The national security letter is not only **among the most highly regulated things the FBI does**, but a very important building block tool of our national security investigations,” Comey

said. "What worries me about their suggestion that we impose a judicial procedure on NSLs, is that it would actually make it harder for us to do national security investigations than bank fraud investigations."

Comey said applying to a judge for a letter to track down an internet user who made a post indicating an interest in carrying out a terrorist bombing would take days or perhaps weeks, even if more judges were added to the court.

"Being able to do it in a reasonably expeditious way is really important to our investigations. So one of my worries about the proposal in the review group is it would add or introduce a delay," he said. The director did say he believed there was merit to the review panel's suggestion that such national security letters not come with a permanent bar on the recipient discussing the order with anyone other than legal counsel.

"We ought to be able to work something out that adopts a nondisclosure regime that is more acceptable to a broader array of folks than the one we have now," he said.

Comey acknowledged that the FBI process for issuing such letters was too lax several years ago, but insisted **it has since been fixed and is now rigorous and heavily audited**. "No doubt the process for NSLs was broken in some ways six years ago or longer. It is not broken today. And so I don't know why we would make natioanls [sic] security investigations harder in that respect than criminal investigations," he said. He also said doing so would likely encourage his agents to go through prosecutors to get a grand jury subpoena instead—a process that doesn't require

the same number of approvals. [my emphasis]

Here's the problem with this (aside from the hilarious claims that a program with no external oversight is the most "highly regulated" thing the FBI does, as bolded).

The journalists all, without an exception I've found, permitted Comey to misrepresent the Review Group's two recommendations pertaining to National Security Letters (though HuffPo did include additional reporting noting that two of the Review Group members were Comey's law professors and he thinks their emphasis is on gag orders preventing recipients from discussing the orders).

I described what the Review Group's NSL recommendations were here (Julian Sanchez also did a good post).

But to understand why this is important enough for me to be an asshole over, it helps to see Review Group Recommendation 1, affecting the Section 215 dragnet, next to Review Group Recommendation 2, affecting NSLs.

Recommendation 1

We recommend that section 215 should be amended to authorize the Foreign Intelligence Surveillance Court to issue a section 215 order compelling a third party to disclose otherwise private information about particular individuals only if [it finds that

(1)] the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities" and

(2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 2

We recommend that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that:

(1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and

(2) like a subpoena, the order is reasonable in focus, scope, and breadth.

[punctuation and spacing altered in brackets]

That is, Recommendation 1 (affecting Section 215) and Recommendation 2 (affecting NSLs) are – in the clauses changing the standard of review to eliminate bulk collection – substantively **exactly the same**. And while the NSLs require judicial review to **get** to any enforceable of standard of review – which is definitely one huge proposed change to the NSLs – viewed together like this, it is clear that at least as significant a goal of the Review Group is to end bulk collection under any authority.

Particularly when you consider Recommendation 3, which recommends real minimization procedures for NSLs.

The Review Group recommended judicial review of NSLs, sure. But it also recommended either preventing or (given the likelihood this has been going on) eliminating bulk collection.

And yet a room full of – in some cases – very good journalists allowed the FBI Director to criticize what they all reported as the Review

Group's recommendation that NSL's undergo judicial review without even mentioning he misrepresented the recommendation, addressing only a fraction of what the Review Group recommended.

Now maybe I'm wrong and the Review Group is not at all concerned about NSL bulk collection in spite of recommending eliminating it as their second recommendation. Maybe the voracious journalist-eating FBI Director really is concerned exclusively about judicial review (and willing to budge on gag orders).

Except by ignoring the bulk collection recommendation pertaining to NSLs, the journalists have allowed the Administration to eliminate the most important part of this debate.

Already, the press is portraying the resolution of the Section 215 collection as a decision between third party retention and telecom retention (with AT&T and Verizon still holding and being able to contact-chain most calls that occur in the country). When you combine that with the complete silence about the recommendation that bulk NSLs be eliminated, the journalists are not mentioning that the Administration's proposed solutions for the phone dragnet (third party or telecom) and for NSLs (no change) preserve most of the aspects of bulk collection.

Jim Comey invited journalists from the nation's top media outlets in for lunch, and he ate them for lunch them on bulk collection. With the result that the Review Group's (and Leahy-Sensenbrenner's) central recommendation to eliminate dragnets has all but disappeared from discussions of what will happen to the dragnet.

Update: See NSArchive's call for NSL reform.

JOHN INGLIS EXPLAINS WHY (US-BASED COLLECTION OF) INTERNET METADATA DOESN'T WORK

Steve Inskeep got a very long interview with NSA Deputy Director John Inglis. It suffers from the same problem that just about every interview the NSA has done since the Snowden leaks started has – because the NSA will only allow friendlies or non-beat writers to do interviews, NSA can avoid many real questions and falsely represent the facts (such as, just one example, what the Review Group really said about the legality of NSA's programs).

But Inskeep did a good job, and succeeded in doing something that no one else has: get a real explanation for why the NSA gave up its (US-based collection of) Internet “metadata.”

Inskeep starts by suggesting NSA was unable to meet the requirements of the program. But Inglis insists that wasn't the problem. Rather, it was that Internet companies keep no billing records for individual emails.

INSKEEP: And it was abandoned because it was too hard to comply with the safeguards and because it was judged not to be practical, it wasn't worth the cost.

INGLIS: It was abandoned principally for the latter reason, which is it was just too hard to make operationally workable. In theory, and especially given that people move more and more to emails, right, that kind of communication, in theory it would be even more valuable to try to detect a plot that moves from a foreign domain to a domestic domain using email metadata. The challenge is,

is that the business model within the private sector doesn't support that. You and I grew up in an America where there were local calls, long distance calls, and the telephone company made their money by charging you for the number of local calls or the number of long distance calls for some duration. And for that reason they tracked that information. You could go to the telephone company and say, how many calls and what number called what number.

And they would actually track that with great precision. Email didn't get its start that way. The first email account I had from a company with three letters said, for \$6.95 a month you can write a million emails or one email, we don't care. We're going to send you, sell you a bandwidth. And so there was no material business interest on their part to track the metadata. They just wanted to sell you access to the pipe. Given that that information it doesn't exist, it's hard to recreate it. It became operationally very difficult to do that. It is theoretically possible, but very expensive. And we've decided in late 2011 that while we thought we could meet the requirements of the court, we were quite confident that we could, the only way we could proceed was in so doing, that it was operationally too difficult to do that because the business model was so different.

Ultimately, of course, Inglis is confirming Inskip's first assertion: that the NSA couldn't meet the Court's requirements that it not collect content that is also routing information, because the telecoms, from which NSA collected this data, only had access to the data the NSA wanted at a content level.

NSA could meet FISC's requirements. But to do so

gave them little meaningful data, because the telecom level of content isn't all that useful.

Of course, they can collect that data elsewhere, in places where such content-based restrictions aren't in place.

AFTER MEETING WITH OBAMA, BOB GOODLATTE CALLS FOR REFORM OF PHONE DRAGNET

Bob Goodlatte, the Chair of the House Judiciary Committee, voted against the Amash-Conyers Amendment that would have defunded the phone dragnet. Nor is he a named cosponsor of the USA Freedom Act, the Leahy-Sensenbrenner bill that would reform the dragnet.

Which is why it is particularly notable that he's the one member of Congress cited by name in a story reporting on skepticism that Obama will actually reform the NSA.

President Obama met with hand-picked lawmakers at the White House on Thursday to discuss the National Security Agency's controversial spying programs, the main event of a week full of meetings at the White House focusing on potential reforms for the maligned federal agency.

[snip]

At least some of the lawmakers left the meeting unconvinced that the president is going to do enough to curtail the NSA's activities. House Judiciary Committee Chairman Bob Goodlatte, R-Va.,

said "it's increasingly clear that we need to take legislative action to reform" the NSA's intelligence gathering.

"If the president believes we need a bulk collection program of telephone data, then he needs to break his silence and clearly explain to the American people why it is needed for our national security," Goodlatte said in a statement. "Americans' civil liberties are at stake in this debate."

If the President has not yet been able to convince Goodlatte the phone dragnet is necessary, if Goodlatte walks out of meeting with the President calling to legislatively roll back the phone dragnet, it might just have a shot at passing.

Update: Here's Goodlatte's full statement.

Over the course of the past several months, I have urged President Obama to bring more transparency to the National Security Agency's intelligence-gathering programs in order to regain the trust of the American people. In particular, if the President believes we need a bulk collection program of telephone data, then he needs to break his silence and clearly explain to the American people why it is needed for our national security. **The President has unique information about the merits of these programs and the extent of their usefulness.** This information is critical to informing Congress on how far to go in reforming the programs. Americans' civil liberties are at stake in this debate.

With each new revelation of the scope of these programs, it's increasingly clear that we need to take legislative action to reform some of our nation's

intelligence-gathering programs to ensure that they adequately protect Americans' civil liberties and operate in a sensible manner. We also need to ensure the laws are clear so that the U.S. tech industry is not disadvantaged vis-à-vis their foreign competitors. The House Judiciary Committee, which has primary jurisdiction over the legal framework of these programs, has conducted aggressive oversight on this issue and will be instrumental to reforming the Foreign Intelligence Surveillance Act. I am committed to working with members of Congress and Senators from both political parties, House leaders, and President Obama to ensure our nation's intelligence collection programs include real protections for Americans' civil liberties, robust oversight, and additional transparency. [my emphasis]

THE FBI (OR NSA?)'S BULK NATIONAL SECURITY LETTERS

Say, did you notice that the NSA Review Group, like the Leahy-Sensenbrenner bill before it, endorsed dramatic restrictions on National Security Letters?

Both efforts set out to address the most extreme privacy risks posed by – the perception was – the NSA, yet both would impose new rules on NSLs, which are primarily used by the FBI. And both efforts would attempt to at least limit (and therefore presumably end) any bulk

collection with NSLs.

Leahy-Sensenbrenner provides specific changes to both the statute authorizing communications collection and the one authorizing financial data collection. In the case of toll records, the changes look like this:

Required Certification.— The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director may request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(1) the name, address, length of service, and toll billing records sought are relevant **and material** to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States; and

(2) there are **reasonable grounds to believe that the name, address, length of service, and toll billing records sought pertain** to—

(A) a foreign power or agent of a foreign power;

(B) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

(C) an individual in contact with, or known to, a suspected agent of a foreign

power. [my emphasis]

In addition, Leahy-Sensenbrenner would make NSL gags harder to sustain.

The Review Group went even further with respect to the basic NSL requests. It recommended (as its 2nd and 3rd recommendations, stuck right in the middle of its Section 215 discussion!) not only limiting bulk collection with NSLs, but requiring judicial review and adding minimization procedures to them.

Recommendation 2 We recommend that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that:

(1) the government **has reasonable grounds to believe that the particular information sought** is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and

(2) like a subpoena, **the order is reasonable in focus, scope, and breadth.**

Recommendation 3 We recommend that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders.
[my emphasis]

There are two possible reasons why Leahy-Sensenbrenner and the Review Group would offer such similar reforms. First, it’s possible they worry that limiting bulk collection on Section 215 without limiting it on NSLs would lead the government to use NSLs instead.

Far more likely, both would propose such reforms

because they know NSLs **had already been used** for bulk collection. (We know DOJ used bulk NSLs in its efforts to fix its exigent letter problems, but that involved just 3 bulk orders, all 3 issued in 2006.)

Which would be alarming because – as the Review Group points out – in FY2012 (which extends from October 1, 2011 to September 30, 2012), the FBI issued 21,000 NSLs, “primarily for subscriber information.” DOJ’s reports to Congress reported 16,511 NSL requests in 2011 and 15,229 in 2012 that weren’t subscriber information only, so roughly 5,500 of that 21,000 were just subscriber information. But the FBI could very well be issuing bulk orders for both toll records and financial records.

That’s a lot of potential bulk orders.

And, as the Review Group makes clear in its list of reasons the NSLs are ripe for abuse, the FBI doesn’t treat this data with the same care that NSA purportedly treats the phone dragnet data.

[T]he oversight and minimization requirements governing the use of NSLs are much less rigorous than those imposed in the use of section 215 orders.

So data from potentially thousands of bulk orders, covering both toll and financial records, may be sitting on FBI’s servers, with few access, dissemination, and age-off restrictions.

No wonder the Review Group thinks the NSLs should be subject to the same kind of judicial scrutiny as the other laws repurposed for bulk collection.

There is one final—and important— issue about NSLs. For all the well-established reasons for requiring neutral and detached judges to decide when government investigators may invade an individual’s privacy, there is a strong

argument that NSLs should not be issued by the FBI itself. Although administrative subpoenas are often issued by administrative agencies, foreign intelligence investigations are especially likely to implicate highly sensitive and personal information and to have potentially severe consequences for the individuals under investigation. We are unable to identify a principled reason why NSLs should be issued by FBI officials when section 215 orders and orders for pen register and trap-and-trace surveillance must be issued by the FISC.

Which is precisely the reason why the Administration is fighting this.

While the focus on reforms Obama may reject has centered on the phone dragnet collection, anonymous sources are also saying the government can't accept the Review Group proposal for NSLs.

Civil liberties groups would like Obama to rein in the government's use of so-called "national security letters," which allow the FBI and other agencies to compel individuals and organizations to turn over **business** records without any independent or judicial review.

A senior administration official said no final decisions had been made yet, but some operational agencies have concerns about limiting the use of these letters because it would raise the bar for intelligence investigations above that for criminal ones.

Which is understandable, so long as you ignore the high likelihood these are bulk orders. But once you imagine how many Americans' records this might include if any significant number of NSLs are bulk orders, then it seems utterly shocking no judge reviews the requests.

That's presumably one of the reasons the Administration wants to rush through its recommendations before we think too hard about the implications of bulk NSL orders.

SUCKY ASSESSMENTS OF THE PHONE DRAGNET REVEAL HOW MUCH THEY'RE KEEPING "SECRET"

The assessments of the phone dragnet suck.

I don't mean the assessments of the phone dragnet show the program sucks, though that may well be the case. I mean the assessments of the phone dragnet I've seen do a very poor job of assessing the value of it. Which serves to show how much of the larger dragnet remains, if not secret, still largely undiscussed.

To see what I mean, consider this post, from Just Security's Ryan Goodman.

Insiders disagree about the phone dragnet value with outsiders

The strongest part of his post compares the seemingly contradictory assessments of the phone dragnet by two different members of the NSA Review Group. University of Chicago Professor Geoffrey Stone and Deputy Director of CIA Mike Morell.

Stone, based on what he learned from public sources and from the briefings the Group received, believes the program did not prevent any terrorist attacks. Morell, whose former agency receives Tippers from the program and even had direct access to query results until 2009 just like the FBI does and did (though no

one talks about that) insists it has helped prevent terrorist attacks.

Goodman also notes that the Gang of Four immediately defended the phone dragnet after the Review Group released its results (actually, they object to more than the phone dragnet recommendation but don't say what other recommendations they object to), but doesn't note the terms they use to do so:

However, a number of recommendations in the report should not be adopted by Congress, starting with those based on the misleading conclusion that the NSA's metadata program is 'not essential to preventing attacks.' **Intelligence programs do not operate in isolation** and terrorist attacks are not disrupted by the work of any one person or program. The NSA's metadata program is a valuable analytical tool that assists intelligence personnel in their efforts to efficiently 'connect the dots' on emerging or current terrorist threats directed against Americans in the United States. **The necessity of this program cannot be measured merely by the number of terrorist attacks disrupted, but must also take into account the extent to which it contributes to the overall efforts** of intelligence professionals to quickly respond to, and prevent, rapidly emerging terrorist threats. [my emphasis]

In other words, Goodman presents evidence that the Gang of Four and a former top CIA official believe there are other reasons the phone dragnet is valuable, while someone relying on limited briefings evaluates the program based on its failure to stop any attack.

That ought to make Goodman ask what Morell and Dianne Feinstein know (or think they know) that Stone does not. It ought to make him engage seriously with their claim that **the phone**

dragnet is doing something else beyond providing the single clues to prevent terrorist attacks.

One they're not willing to talk about explicitly.

Assessments and the terrorist attack thwarted metric

Instead, Goodman assesses the phone dragnet solely on the basis of the public excuse offered over and over and over since the Guardian first published the Verizon order in June: to see which Americans are in contact with (alleged) terrorist associates so as to prevent an attack.

Goodman lectures program critics that identifying funders or members of terrorist groups might help find terrorists, too, and "peace of mind" might help dedicate resources most productively.

The key objective of course is to stop terrorist attacks against the US homeland and vital US interests abroad. An important distinction, however, is whether the intelligence generated by the program is:

(a) "direct": timely information to foil a specific attack; or

(b) "indirect": information that enables the government to degrade a terrorist group or decrease the general likelihood of attacks

Examples of the latter might include information on individuals who have joined or are funding a terrorist organization. Intelligence could help to identify and successfully prosecute such individuals, and hence disable them and deter others. The important point is that both types of information aid the overall goal of stopping terrorist attacks. That point appears to have been lost on some critics of the program. When the government cites the latter

information yields, critics often consider such situations irrelevant or little to do with stopping attacks.

But Goodman imagines only those affirmatively supporting terrorism would help the government prevent terrorism, which is not necessarily the case.

Does the NSA's network analysis even pick the right calls?

One thing missing from such assessments are the failures. Why didn't, for example, Faisal Shahzad's planning with the Pakistani Taliban identify him and his *hawala* before the attack? There are plausible explanations: he used good enough operational security such that he had no communications that could have included in the dragnets, his TTP phone and Internet contacts were not among the services sucked up, the turmoil in the phone and (especially) Internet dragnet in 2009 and 2010 led to gaps in the collection. Then there's a far more serious one: that the methods NSA use to identify numbers of interest may not work, and may instead only be identifying those whose doings with terror affiliates are relatively innocent, meaning they don't use operational security (though note the US-based phone dragnets would use more sophisticated analysis only after data gets put in the corporate store, whereas data collected overseas might be immediately subject to it).

And for those who, like Goodman, place great stock in the dragnet's "peace of mind" metric, they need to assess not just the privacy invasion that might result, but the resources required to investigate all possible leads – which could have been upwards of 36,000 people in the Boston Marathon case.

That is, unless we have evidence that NSA's means of picking the interesting phone contacts from the uninteresting ones works (and given the numbers involved, we probably don't have that), then the dragnet may be as much a time suck as

it is a key tool.

What about the other purposes the Intelligence Community has (quietly) admitted?

The other problem with assessments of the phone dragnet is they don't even take the IC at its word in its other, quieter admissions of how it uses the dragnet (notably, in none of Stone's five posts on the dragnet does he mention any of these – one, two, three, four, five – raising questions whether he ever learned or considered them). These uses include:

- Corporate store
- “Data integrity” analysis
- Informants
- Index

Corporate store: As the minimization procedures and a few FISC documents make clear, once the NSA has run a query, the results of that query are placed in a “corporate store,” a database of all previous query results.

ACLU's Patrick Toomey has described this in depth, but the key takeaways are once data gets into the corporate store, NSA can use “the full range of SIGINT analytic tradecraft” on it, and none of that activity is audited.

NSA would have you believe very few Americans' data gets into that corporate store, but even if the NSA treats queries it says it does, it could well be in the millions. Worse, if NSA doesn't do what they say they do in removing high volume numbers like telemarketers, pizza joints, and cell voice mail numbers, literally everyone could be in the corporate store. As far as I've seen, the metrics measuring the phone dragnet only involve tips **going out** to FBI and not the gross number of Americans' data going into the corporate store and therefore subject to “the full range of analytic tradecraft,” so we (and probably even the FISC) don't know how many Americans get sucked into it. Worse, we don't know what's included in “the full range of

SIGINT analytic tradecraft" (see this post for some of what they do with Internet metadata), but we should assume it includes the data mining the government says it's not doing on the database itself.

The government doesn't datamine phone records in the main dragnet database, but they're legally permitted to datamine anyone's phone records who has come within 3 degrees of separation from someone suspected of having ties to terrorism.

"Data integrity" analysis: As noted, the NSA claims that before analysts start doing more formal queries of the phone dragnet data, "data integrity" analysts standardize it and do something (it's unclear whether they delete or just suppress) "high volume numbers." They also – and the details on this are even sketchier – use this live data to develop algorithms. This has the possibility of significantly changing the dragnet and what it does; at the very least, it risks eliminating precisely the numbers that might be most valuable (as in the Boston Marathon case, where a pizza joint plays a central role in the Tsarnaev brothers' activities). The auditing on this activity has varied over time, but Dianne Feinstein's bill would eliminate it by statute. Without such oversight, data integrity analysts have in the past, moved chunks of data, disaggregated them from any identifying (collection date and source) information, and done ... we don't know what with it. So one question about the data integrity analyst position is how narrowly scoped the high volume numbers are (if it's not narrow, then everyone's in the corporate store); an even bigger is what they do with the data in often unaudited behavior before it's place into the main database.

Informants: Then there's the very specific, admitted use of the dragnet that no one besides me (as far as I know) has spoken about: to find potential informants. From the very start of the FISC-approved program, the government maintained the dragnet "may help to discover individuals

willing to become FBI assets," and given that the government repeated that claim 3 years later, it does seem to have been used to find informants.

This is an example of a use that would support "connecting the dots" (as the program's defenders all claim it does) but that could ruin the lives of people who have no tie to actual terrorists (aside from speaking on the phone to someone one or two degrees away from a suspected terror affiliate). The government has in the past told FISC it might use FISA data to find evidence of other crimes – even rape – to coerce people to become informants, and in some cases, metadata (especially that in the corporate store, enhanced by "the full range of analytic tradecraft") could pinpoint not just potential criminals, but people whose visa violations and extramarital affairs might make them amenable to nancing on the people in their mosque (with the additional side effect of building distrust within a worship community). There's not all that much oversight over FBI's use of informants in any case (aside from permitting us to learn that they're letting their informants commit more and more crimes), so it's pretty safe to assume no one is tracking the efficacy of the informants recruited using the powerful tools of the phone dragnet.

Index: Finally, there's the NSA's use of this metadata as a Dewey Decimal System (to use James Clapper's description) to pull already-collected content off the shelf to listen to – a use even alluded to in the NSA's declarations in suits trying to shut down the dragnet.

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]

Don't get me wrong. Given how poorly the NSA has addressed its longterm failure to hire enough translators in target languages, I can understand how much easier it must be to pick what to read based on metadata analysis (though see my concerns, above, about whether the NSA's assessment techniques are valid). But when the NSA says, "non-US persons" here, what they mean is "content collected by targeting non-US persons," which includes a great deal of content of US persons.

Which is another way of saying the dragnet serves as an excuse to read US person content.

And however valuable (or, given the NSA's other failures) necessary that may be, that also opens up a whole new way in which this dragnet infringes on US person privacy. Indeed, "reading already-collected content" almost certainly falls under "the full range of SIGINT analytic tradecraft," which may mean that being caught up in the phone dragnet equates to having your content either back door targeted or reverse targeted. Does the NSA read such indexed content before it sends tips out to the FBI to "start" an investigation? How much does the NSA learn from listening to calls between journalists or ACLU lawyers and people 2 degrees away from terror affiliates?

Now, frankly, all four of these admitted uses of the dragnet might be used to support defenders' or opponents' claims about the dragnet. All of them raise big new privacy concerns (which is surely why the defenders have never laid this out). But they might well provide information that is far more valuable in stopping terror attacks than the phone record of Basaaly Moalin's 2-degree phone contact with Aden Ayro was.

The point is, no one is talking about these uses of the dragnet. No one. And until they do, commentators shouldn't be lecturing anyone about the adequacy or inadequacy of their dragnet assessment.

Of course, one reason we're not talking about all this is because the program defenders don't want to (I'm certain, for example, that one of the other NSA Group Recommendations the Gang of Four opposes is the requirement of warrants for back door searches, but they won't say that out loud). We don't know the full details of these uses, because they're still shrouded in secrecy. It's not even clear that all members of the NSA Review Group learned full details about them.

Perhaps, then, before people write anymore long posts claiming to assess the phone dragnet, they should be insisting on answers to a lot more questions?

The NSA and its defenders have gone to great lengths to prevent the public from conducting real assessments of the phone dragnet's efficacy. That, by itself, should raise concerns. But it should also make it clear that current assessments are just scratching the surface.

OBVIOUSLY BOGUS CLAPPER EXONERATION ATTEMPT 4.0

[youtube]QwiUVUJmGjs[/youtube]

Wyden: Does the NSA collect any type of data, at all, on millions, or hundreds of millions of Americans?

Clapper: No sir.

Wyden: It does not?

Clapper: There are cases where they could inadvertently, perhaps, uh, collect, but not wittingly. [After 6:38]

Almost immediately after the first Edward Snowden leaks proved James Clapper lied when he told Ron Wyden the NSA doesn't collect data of any kind on millions of Americans, Clapper explained that he meant the NSA didn't vicariously pore through Americans' emails.

"What I said was, the NSA does not voyeuristically pore through U.S. citizens' e-mails. I stand by that," Clapper told National Journal in a telephone interview.

That is, his first response was about reading emails in a certain smarmy fashion; he did not apparently deny collecting them.

Then, with a bit more time to think up an excuse, he admitted to Andrea Mitchell that he had been "too cute by half" but didn't really explain what semantic excuse he had invented for himself.

First— as I said, I have great respect for Senator Wyden. I thought, though in retrospect, I was asked— "When are you going to start— stop beating your wife" kind of question, which is meaning not—

answerable necessarily by a simple yes or no. So **I responded in what I thought was the most truthful, or least untruthful manner** by saying no.

[snip]

And this has to do with of course somewhat of a semantic, perhaps some would say too— **too cute by half**. But it is— there are honest differences on the semantics of what— when someone says “collection” to me, that has a specific meaning, which may have a different meaning to him. [my emphasis]

Nevertheless, the implication, less than a week after Snowden’s first revelations, was that collecting Americans’ metadata doesn’t count until you access it, which seems to address the phone dragnet data (though would apply to incidentally collected US person data as well).

Perhaps because his Mitchell answer only increased the mockery, Clapper thought up a new answer, one he sent Senate Intelligence Committee Chair Dianne Feinstein 3 months after he lied to her committee.

I have thought long and hard to re-create what went through my mind at the time. In light of Senator Wyden’s reference to “dossiers” and faced with the challenge of trying to give an unclassified answer about our intelligence collection activities, many of which are classified, **I simply didn’t think of Section 215 of the Patriot Act.** Instead, my answer addressed collection of the content of communications. I focused in particular on Section 702 of FISA, because we had just been through a year-long campaign to seek reauthorization of this provision and had had many classified discussions about it, including with Senator Wyden. That is why I added a comment about

“inadvertent” collection of U.S. person information, because that is what happens under Section 702 even though it is targeted at foreigners.

That said, **I realized later** that Senator Wyden was asking about Section 215 metadata collection, rather than content collection. Thus, my response was clearly erroneous—for which I apologize. While **my staff acknowledged the error to Senator Wyden’s staff soon after the hearing**, I can now openly correct it because the existence of the metadata collection program has been declassified. [my emphasis]

Note Clapper himself admits he spent time (and he suggests, though it’s not entirely clear, that it continued up to June) trying to think through what he had said. He also didn’t acknowledge that Wyden’s office had to call him on his lie. Which of course means he doesn’t say specifically what Wyden’s office said after he lied blatantly.

Clapper’s changing answers have only fed the impression (supported by many other Clapper comments) that he’s a liar. Which is probably why the NYT called him one in its call for amnesty for Edward Snowden.

Clapper’s office, however, has not given up hope of convincing us he’s not a liar. Today, ODNI General Counsel Robert Litt tried to refute the NYT’s claim he’s a liar.

“Edward Snowden, Whistle-Blower” (editorial, Jan. 2) repeats the allegation that James R. Clapper Jr., the director of national intelligence, “lied” to Congress about the collection of bulk telephony metadata. **As a witness to the relevant events and a participant in them, I know that allegation is not true.**

Senator Ron Wyden asked about collection

of information on Americans during a lengthy and wide-ranging hearing on an entirely different subject. **While his staff provided the question the day before, Mr. Clapper had not seen it.** As a result, **as Mr. Clapper has explained, he was surprised by the question and focused his mind on the collection of the content of Americans' communications.** In that context, his answer was and is accurate.

When we pointed out Mr. Clapper's mistake to him, he was surprised and distressed. I spoke with a staffer for Senator Wyden several days later and told him that although Mr. Clapper recognized that his testimony was inaccurate, it could not be corrected publicly because the program involved was classified.

This incident shows the difficulty of discussing classified information in an unclassified setting and **the danger of inferring a person's state of mind from extemporaneous answers given under pressure.** Indeed, it would have been irrational for Mr. Clapper to lie at this hearing, since every member of the committee was already aware of the program. [my emphasis]

As a threshold matter, when a crafty lawyer like Litt says his principal did not "see" the question, it says nothing about whether or not Clapper "knew" about the question. Usually, senior officials get briefed on such things, they don't read them. Though they presumably are more likely to read letters from members of Congress, and Clapper had received and not fully responded to several related letters from Wyden already by that point, including some invoking Keith Alexander's earlier lies about collection on US persons.

Which is one reason I'm intrigued that Litt

seems to have added the claim that Clapper was “surprised” to the public record – I’m not aware of Clapper ever expressing such a thing. If he were surprised, it’d be especially problematic given his involvement in correspondence going back months.

But that “surprised” (apparent) invention allows Litt to claim that Clapper didn’t know what he was answering when he almost certainly did, given that he had been avoiding answering that question in unclassified form for months.

More interesting still is Litt’s warning about inferring a person’s state of mind. Clapper himself said he thought long and hard, three months after his lies, to recreate what he was thinking at the time. So how can Litt claim to know that Clapper didn’t lie, based on an assertion about what he was thinking (unless he told him what he was thinking, which I guess crafty lawyers do sometimes)?

Here’s the other thing. Perhaps Wyden was thinking only of one (the secret phone dragnet collecting data on hundreds of millions of Americans) or the other (the mostly unacknowledged backdoor searches on content collected “incidentally” on millions of Americans) NSA collection of any kind of data on millions of Americans. But his conversations have often linked the two (perhaps because the Intelligence Community uses metadata in part to decide which Americans’ content to go read without RAS?). And he might well be including the **intentional** collection of US person data via upstream collection (though there’s no reason to believe that includes millions of Americans).

But even if he was asking about incidentally collected (and then back door searched) US person data, Clapper’s first instinct was a flat “no.” It wasn’t until Wyden challenged him with the mock surprise he has had so much practice at affecting, “it does not?,” that Clapper retreated to his “wittingly” lie. And “wittingly” – even “inadvertently” – are different words than “incidentally.” One point

of this Section 702 is to collect the contacts of suspected terrorists, including the Americans. That's the intent; there's nothing inadvertent about it (as people like Sheldon Whitehouse have made clear).

Moreover, Clapper's first response – that they don't voyeuristically read the emails they collect – assumes they do collect them. His first response assumes they intentionally collect content, but don't necessarily access them all.

The NSA collects the content of millions of Americans "incidentally" (using their official euphemism), but there's nothing unintentional or inadvertent or unwitting about that collection.

Even this fall-back lie is demonstrably a lie.

So nice of Robert Litt to confirm the NYT's impressions on their Letters-to-the-Editors page.

Update: You've got a "pal" in principal error corrected per BS.