THE GOVERNMENT HAS A FESTERING EO 12333 PROBLEM IN JEWEL/FIRST UNITARIAN

The government claims it does not have a protection order pertaining to the phone dragnet lawsuits because the suits with a protection order pertain only to presidentially-authorized programs.

> The declaration made clear, in a number of places, that the plaintiffs challenged activities that occurred under presidential authorization, not under orders of the Foreign Intelligence Surveillance Court (FISC), and that the declaration was therefore limited to describing information collected pursuant to presidential authorization and the retention thereof.

Therefore, the government is challenging the EFF's effort to get Judge Jeffrey White to reaffirm that the preservation orders in the Multidistrict Litigation and Jewel apply to the phone dragnet.

Fine. I think EFF can and should challenge that claim.

But let's take the government at its word. Let's consider what it would obliged to retain under the terms laid out.

The government agrees it was obliged, starting in 2007, to keep the content and metadata dragnets that were carried out exclusively on presidential authorization. Indeed, the declaration from 2007 they submitted describing the material they've preserved includes telephone metadata (on tapes) and the queries of metadata, including the identifiers used (see PDF 53). It also claimed it would keep the

reports of metadata analysis.

That information is fundamentally at issue in First Unitarian Church, the EFF-litigated challenge to the phone dragnet. That's true for three reasons.

First, the government makes a big deal of their claim, made in 2007, that the metadata dragnet databases were segregated from other programs. Whether or not that was a credible claim in 2007, we know it was false starting in early 2008, when "for the purposes of analytical efficiency," a copy of that metadata was moved into the same database with the metadata from all the other programs, including both the Stellar Wind phone dragnet data, and the ongiong phone dragnet information collected under EO 12333.

And given the government's promise to keep reports of metadata analysis, from that point until sometime several years later, it would be obliged to keep all phone dragnet analysis reports involving Americans. That's because — as is made clear from this Memorandum of Understanding issued sometime after March 2, 2009 — the analysts had no way of identifying the source of the data they were analyzing. The MOU makes clear that analysts were performing queries on data including "SIGINT" (EO 12333 collected data), [redacted] — which is almost certainly Stellar Wind, BRFISA, and PR/TT. So to the extent that any metadata report didn't have a clear time delimited way of identifying where the data came from, the NSA could not know whether a query report came from data collected solely pursuant to presidential authorization or FISC order. (The NSA changed this sometime during or before 2011, and now metadata all includes XML tags showing its source; though much of it is redundant and so may have been collected in more than one program, and analysts are coached to re-run queries to produce them under EO 12333 authority, if possible.)

Finally, the real problem for the NSA is that the data "alerted" illegally up until 2009 —

including the 3,000 US persons watchlisted without undergoing the legally required First Amendment review — was done so precisely because when NSA merged its the phone dragnet data with the data collected under Presidential authorization — either under Stellar Wind or EO 12333 — it applied the rules applying to the presidentially-authorized data, not the FISC-authorized data. We know that the NSA broke the law up until about 5 years ago. We know the data from that period — the data that is under consideration for being aged off now — broke the law precisely because of the way the NSA mixed EO 12333 and FISC regulations and data.

The NSA's declarations on document preservation — not to mention the declarations about the dragnets more generally — don't talk about how the EO 12333 data gets dumped in with and mixed up with the FISC-authorized data. That's NSA's own fault (and if I were Judge White it would raise real questions for me about the candor of the declarants).

But since the government agreed to preserve the data collected pursuant to presidential authorization without modification (without, say, limiting it to the Stellar Wind data), that means they agreed to preserve the EO 12333 collected data and its poisonous fruit which would just be aging off now.

I will show in a follow-up post why that data should be utterly critical, specifically as it pertains to the First Unitarian Church suit.

But suffice it to say, for now, that the government's claim that it is only obliged to retain the US person data collected pursuant to Presidential authorization doesn't help it much, because it means it has promised to retain all the data on Americans collected under EO 12333 and queries derived from it.

THE CLEAR PRECEDENT FOR CARRIE CORDERO'S "UNCHARTED TERRITORY" OF DESTRUCTION OF EVIDENCE

Shane Harris has a report on the government's odd behavior in regards to preserving the phone dragnet data in light of the suits challenging its legality.

It's surprising on three counts. First, because he claims the legal back and forth has not previously been reported.

> Now, that database will include phone records that are older than five years — not exactly the outcome that critics of the NSA program were hoping for. A dramatic series of legal maneuvers, which have not been previously reported, led the outcome.

It's surprising not just because the "legal maneuvers" have in fact been reported before (though not the detail that James Cole got involved, though it's not yet clear how his involvement affected the actual legal maneuvers rather than the internal DOJ communication issues). But also because Harris neglects to mention key details of those legal maneuvers — notably that EFF reminded DOJ, starting on February 26, that it had preservation orders that should affect the dragnet data, reminders which DOJ stalled and then ignored.

Harris' piece is also surprising because of the implicit suggestion that NSA hasn't been aging off data regularly, as it is supposed to be.

> A U.S. official familiar with the legal process said the question about what to

> do with the phone records needn't have been handled at practically the last minute. "The government was coming up on a five-year deadline to delete the data. Lawsuits were pending. The Justice Department could have approached the FISC months ago to resolve this," the official said, referring to the Foreign Intelligence Surveillance Court.

There should be no "deadline" here — aside from the daily "deadline" that should automatically age off the five year old data. Now, the WSJ had previously reported that that's not actually how age-off works.

> As the NSA program currently works, the database holds about five years of data, according to officials and some declassified court opinions. About twice a year, any call record more than five years old is purged from the system, officials said.

But even assuming NSA only ages off data twice a year (in which case they should stop claiming they only "keep" data for 5 years because they already keep some of it for 5 1/2 years), most of these suits are well older than 6 months old, predating what might have been an August age-off, which means unless NSA already deviated from its normal pattern, it deleted data relevant to the suits.

By far the most surprising detail in Harris' story, however, is this response from former DOJ National Security Division Counsel Carrie Cordero to the news that Deputy Attorney General James Cole has gotten involved. This is, Cordero claims, "uncharted territory."

> "This is all uncharted territory," said Carrie Cordero, a former senior Justice Department official who recently served as the counsel to the head of the National Security Division. "Given the

> complexity and the novelty of this chain of events, it's a good thing that the deputy attorney general is personally engaged, and it demonstrates the significant attention that they're giving to it."

To be more specific about Cordero's work history, from 2007 to 2011, she was deeply involved in FISA-related issues, first at ODNI and then at DOJ's NSD.

> In 2009, I served as Counsel to the Assistant Attorney General for National Security at the Unit ed States Department of Justice, where I co – chaired an interagency group created by the Director of National Intelligence (DNI) to improve FISA processes. From 2007 – 2009, I served in a joint duty capacity as a Senior Associate General Counsel at the Office of the Director of National Intelligence, where I worked behind the scenes on matters relating to the legislative efforts that resulted in the FISA Amendments Act of 2008.

Given her position in the thick of FISA-related issues, one would think she was at least aware of the protection order Vaughn Walker issued on November 6, 2007 ordering the preservation of evidence, up to and including "tangible things," in the multidistrict litigation issues pertaining to the dragnet.

> [T]he court reminds all parties of their duty to preserve evidence that may be relevant to this action. The duty extends to documents, data and tangible things in the possession, custody and control of the parties to this action,

And Cordero presumably should be aware that Walker renewed the same order on November 13, 2009, extending it to cover the Jewel suit, which had an ongoing focus.

Cordero is presumably aware of two other details. First, there should be absolutely no dispute that the phone dragnet was covered by these suits. That's because at least as early as May 25, 2007 (and again in a declaration submitted October 2009), Keith Alexander included the phone dragnet among the things he considered related to the EFF and other suits over which he claimed state secrets.

> In particular, disclosure of the NSA's ability to utilize the TSP (or, therefore, the current FISA Court-authorized content collection) in conjunction with contact chaining [redacted—probably relating to data mining] would severely undermine efforts to detect terrorist activities.
>
> [snip]
>
> To the extent that the NSA's bulk collection and targeted analysis of communication meta data may be at issue in this case, those activities—as described in paragraphs 27 and 28 above—must also be protected from disclosure.

In paragraphs 27 and 28 and the following paragraphs, Alexander named the FISC Pen Register and Telephone Records Orders by name.

Thus, as far back as 2007, the NSA acknowledged that it used its content collection in conjunction with its metadata dragnets, including data obtained pursuant to the FISA dragnet orders.

Furthermore, there should be no dispute that the actual phone records were covered under Walker's order, because the PATRIOT Act Reauthorization of 2005 added the phrase "tangible things" — the very phrase Walker used in his orders — to Section 215.

Finally, there's one more thing Cordero should be aware of, which is why I'm so troubled she

calls this “uncharted territory” (and frankly, why Reggie Walton maybe shouldn’t have been so quick to assume that there were no preservation orders on file). On February 12, 2009, DOJ’s National Security Division told Reggie Walton there was a preservation order that might affect the destruction of the evidence that NSA had been contact chaining in violation of the FISC’s orders, including watchlisting 3,000 US persons with no First Amendment Review.

> With respect to the alert process, after this compliance matter surfaced, NSA identified and eliminated analyst access to all alerts that were generated from the comparison of non-RAS approved identifiers against the incoming BR FISA material. The only individuals who retain continued access to this class of alerts are the Technical Director for NSA’s Homeland Security Analysis Center (“HSAC”) and two system developers assigned to HSAC. From a technical standpoint, NSA believes it could purge copies of any alerts that were generated from comparisons of the incoming BR FISA information against non-RAS approved identifiers on the alert list. However, the Agency, in consultation with DoJ, would need to determine whether such action would conflict with a data preservation Order the Agency has received in an ongoing litigation matter. [my emphasis]

While it appears Cordero had not yet returned to NSD, and therefore there’s no reason to believe she was involved in what increasingly appears to have been a decision to destroy the evidence that NSA violated the clear limits of Section 215 even while people were suing over programs that according to Keith Alexander included Section 215, it is rather surprising that she was unaware of this issue.

And consider the importance of this issue right now.

The NSA and DOJ had a discussion about whether to destroy this evidence that it was violating Section 215 back in February 2009. That data — evidence the NSA broke the law, effectively — would have been aging off just as DOJ decided to claim, again, that these preservation orders dating to 2007 and renewed in 2009 don't protect that evidence that NSA broke the law.

While we can't be certain, by all appearances DOJ decided back in 2009 that those protection orders didn't cover this data. It appears they did destroy the evidence of NSA's law-breaking in 2009. And now we're having a dispute about it again, with central players like Cordero claiming it has never been raised in the past.

Harris' piece describes the need to get James Cole involved as arising from the cumbersome nature of coordinating between the Civil Division (which is managing the lawsuits in which the preservation orders got filed) and the National Security Division (which made the bid with FISC to destroy this data).

> The official noted that the department's National Security Division, which represents the government before the surveillance court, and the Civil Division, which is handling the lawsuits, had to coordinate with each other, and that the back-and-forth has at times been a cumbersome process.
>
> Cole has been acting as a referee between the two sides, and he has made the final decisions on how to proceed with regards to the legal issues presented by the phone records program, the Justice Department official said. The involvement of such a senior official in managing the program underscores the degree to which it has become a particularly nettlesome challenge for the Obama administration to resolve.

But I can't help wondering whether it's not just a cumbersome coordination problem, but incompatible decisions made back in 2007 and 2009. Back in 2007 and 2009, the Civil Division submitted declarations that readily admitted the role of the metadata dragnet in challenged programs (and DOJ lawyer Tony Coppolino has remained intimately involved throughout). Yet between the time when the Civil Division was submitting such declarations in one court (and the court was issuing protection orders), NSD appears to have come to a completely contradictory decision in 2009 to destroy the evidence in question, which presumably should have been covered by the protection order.

Here's the thing: either NSD made what appears to be the clearly correct legal decision in 2009 to retain the evidence NSA violated Section 215, illegally surveilling 3,000 US persons in the 2 1/2 years leading up to 2009, and that data should be noticed to the judge presiding over the EFF suits, Jeffrey White. Or, that evidence of legal wrong-doing got destroyed improperly 5 years ago, and that should be noticed to White. But it sure seems that evidence of illegal watchlisting of 3,000 US persons ought to be relevant to these suits.

THE CLEAR PRECEDENT FOR CARRIE CORDERO'S "UNCHARTED TERRITORY" OF DESTRUCTION OF EVIDENCE

For technical reasons this post has moved here.

IN NOMINATION HEARING, DIRNSA NOMINEE MIKE ROGERS CONTINUES JAMES CLAPPER AND KEITH ALEXANDER'S OBFUSCATION ABOUT BACK DOOR SEARCHES

Yesterday, the Senate Armed Services Committee held a hearing for Vice Admiral Mike Rogers to serve as head of Cyber Command (see this story from Spencer about how Rogers' confirmation as Cyber Command chief serves as proxy for his role as Director of National Security Agency because the latter does not require Senate approval).

Many of the questions were about Cyber Command (which was, after all, the topic of the hearing), but a few Senators asked questions about the dragnet that affects us all.

In one of those exchanges — with Mark Udall — Rogers made it clear that he intends to continue to hide the answers to very basic questions about how NSA conducts warrantless surveillance of Americans, such as whether the NSA conducts back door searches on American people.

> Udall: If I might, in looking ahead, I want to turn to the 702 program and ask a policy question about the authorities under Section 702 that's written into the FISA Amendments Act. The Committee asked your understanding of the legal rationale for NASA [sic] to search through data acquired under Section 702

> using US person identifiers without probable cause. You replied the NASA–the NSA's court approved procedures only permit searches of this lawfully acquired data using US person identifiers for valid foreign intelligence purposes and under the oversight of the Justice Department and the DNI. The statute's written to anticipate the incidental collection of Americans' communications in the course of collecting the communications of foreigners reasonably believed to be located overseas. But the focus of that collection is clearly intended to be foreigners' communications, not Americans. But declassified court documents show that in 2011 the NSA sought and obtained the authority to go through communications collected under Section 702 and conduct warrantless searches for the communications of specific Americans. Now, my question is simple. Have any of those searches been conducted?
>
> Rogers: I apologize Sir, I'm not in a position to answer that as the nominee.
>
> Udall: You–yes.
>
> Rogers: But if you would like me to come back to you in the future if confirmed to be able to specifically address that question I will be glad to do so, Sir.
>
> Udall: Let me follow up on that. You may recall that Director Clapper was asked this question in a hearing earlier this year and he didn't believe that an open forum was the appropriate setting in which to discuss these issues. The problem that I have, Senator Wyden's had, and others is that we've tried in various ways to get an unclassified answer – simple answer, yes or no – to the question. We want to have an answer because it relates – the answer does –

> to Americans' privacy. Can you commit to answering the question before the Committee votes on your nomination?
>
> Rogers: Sir, I believe that one of my challenges as the Director, if confirmed, is how do we engage the American people — and by extension their representatives — in a dialogue in which they have a level of comfort as to what we are doing and why. That is no insignificant challenge for those of us with an intelligence background, to be honest. But I believe that one of the takeaways from the situation over the last few months has been as an intelligence professional, as a senior intelligence leader, I have to be capable of communicating in a way that we are doing and why to the greatest extent possible. That perhaps the compromise is, if it comes to the how we do things, and the specifics, those are perhaps best addressed in classified sessions, but that one of my challenges is I have to be able to speak in broad terms in a way that most people can understand. And I look forward to that challenge.
>
> Udall: I'm going to continue asking that question and I look forward to working with you to rebuild the confidence. [my emphasis]

The answer to the question Rogers refused to answer is clearly yes. We know that's true because the answer is always yes when Wyden, and now Udall, ask such questions.

But we also know the answer is yes because declassified parts of last August's Semiannual Section 702 Compliance Report state clearly that oversight teams have reviewed the use of this provision, which means there's something to review.

> As reported in the last semiannual assessment, NSA minimization procedures now permit NSA to query its databases containing telephony and non-upstream electronic communications using United States person identifiers in a manner designed to find foreign intelligence information. Similarly, CIA's minimization procedures have been modified to make explicit that CIA may also query its databases using United States person identifiers to yield foreign intelligence information. As discussed above in the descriptions of the joint oversight team's efforts at each agency, the joint oversight team conducts reviews of each agency's use of its ability to query using United States person identifiers. To date, this review has not identified any incidents of noncompliance with respect to the use of United States person identifiers; as discussed in Section 4, the agencies' internal oversight programs have, however, identified isolated instances in which Section 702 queries were inadvertently conducted using United States person identifiers. [my emphasis]

It even obliquely suggests there have been "inadvertent" violations, though this seems to entail back door searches on US person identifiers without realizing they were US person identifiers, not violations of the procedures for using back door searches on identifiers known to be US person identifiers.

Still, it is an unclassified fact that NSA uses these back door searches.

Yet the nominee to head the NSA refuses to answer a question on whether or not NSA uses these back door searches.

And it's not just in response to this very basic question that Rogers channeled the dishonest approach of James Clapper and Keith Alexander.

As Udall alluded, at the end of a long series of questions about Cyber Command, the committee asked a series of questions about back door searches and other dragnet issues. They asked (see pages 42-43):

- Whether NSA can conduct back door searches on data acquired under EO 12333 and if so under what legal rationale
- Whether NSA can conduct back door searches on data acquired pursuant to traditional FISA and if so under what legal rationale
- What the legal rationale is for back door searches on data acquired under FISA Amendments Act
- What the legal rationale is for searches on the Section 215 query results in the "corporate store"

I believe every single one of Rogers' answers — save perhaps the question on traditional FISA — involves some level of obfuscation. (See this post for further background on what NSA's Raj De and ODNI's Robert Litt have admitted about back door searches.)

Consider his answer on searches of the "corporate store" as one example.

> What is your understanding of the legal rationale for searching through the "Corporate Store" of metadata acquired under section 215 using U.S. Persons identifiers for foreign intelligence purposes?
>
> The section 215 program is specifically

> authorized by orders issued by the Foreign Intelligence Surveillance Court pursuant to relevant statutory requirements. (Note: the legality of the program has been reviewed and approved by more than a dozen FISC judges on over 35 occasions since 2006.) As further required by statute, the program is also governed by minimization procedures adopted by the Attorney General an d approved by the FISC. Those orders, and the accompanying minimization procedures, require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization specified in the Court's order.

Remember, not only do declassified Primary Orders make it clear NSA doesn't need Reasonable Articulable Suspicion to search the corporate store, but PCLOB has explained the possible breadth of "corporate store" searches plainly.

> According to the FISA court's orders, records that have been moved into the corporate store may be searched by authorized personnel "for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms."71 Analysts therefore can query the records in the corporate store with terms that are not reasonably suspected of association with terrorism. They also are permitted to analyze records in the corporate store through means other than individual contact-chaining queries that begin with a single selection term: because the records in the corporate store all stem from RAS-approved queries, the agency is allowed to apply other analytic methods and techniques to the query results.72 For instance, such

> calling records may be integrated with data acquired under other authorities for further analysis. The FISA court's orders expressly state that the NSA may apply "the full range" of signals intelligence analytic tradecraft to the calling records that are responsive to a query, which includes every record in the corporate store.73

There is no debate over whether NSA can conduct back door searches in the "corporate store" because both FISC and PCLOB say they can.

Which is probably why SASC did not ask whether this was possible — it is an unclassified fact that it is — but rather what the legal rationale for doing so is.

And Rogers chose to answer this way:

1. By asserting that the phone dragnet must comply with statutory requirements
2. By repeating tired boilerplate about how many judges have approved this program (ignoring that almost all of these approvals came before FISC wrote its first legal opinion on the program)
3. By pointing to AG-approved minimization procedures (note—it's not actually clear that NSA's — as distinct from FBI's — dragnet specific procedures are AG-approved, though the more general USSID 18 ones are)

4. By claiming FISA orders and minimization procedures "require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization"

The last part of this answer is either downright ignorant (though I find that unlikely given how closely nominee responses get vetted) or plainly non-responsive. The question was not about queries of the dragnet itself — the "collection store" of all the data. The question was about the "corporate store" — the database of query results based off those RAS approved identifiers. And, as I said, there is no dispute that searches of the corporate store do not require RAS approval. In fact, the FISC orders Rogers points to say as much explicitly.

And yet the man Obama has picked to replace Keith Alexander, who has so badly discredited the Agency with his parade of lies, refused to answer that question directly. Much less explain the legal rationale used to conduct RAS-free searches on phone query results showing 3rd degree connections to someone who might have ties to terrorist groups, which is what the question was.

Which, I suppose, tells us all we need to know about whether anyone plans to improve the credibility or transparency of the NSA.

KEITH ALEXANDER'S ONE STEP SOLUTION

Keith Alexander is testifying before the Senate Armed Services Committee, ostensibly about CyberCommand.

He has gotten a number of questions about the solutions they've offered the President to resolve the phone dragnet issue. He responded it would be possible to keep the data with the telecoms.

Then, in response to a Cyber question, Alexander said the problem is that the NSA can't share classified information about malicious code with industry, because if it does so in a non-classified setting, attackers will learn how NSA obtained the information. (There's a lot that's problematic with that claim, but just ignore all that for now.)

So we need legislation that allows NSA to share classified information back and forth with industry.

He then returned to the phone dragnet. He suggested that the industry retention solution would require legislation allowing NSA to share terrorist identifiers with industry. (Note, this premise is absolutely absurd, as DEA apparently has no problem with sharing drug target identifiers with AT&T in the Hemisphere program in an explicitly unclassified program.)

Finally, he said this legislation — allowing the NSA to share classified identifiers with industry — would serve as the precedent for the Cyber legislation he has long sought but not obtained legislatively.

In other words, on his way out the door, Keith Alexander is now sacrificing his beloved phone dragnet to get cyber legislation in the guise of something else.

NSA'S NEWFOUND CONCERN ABOUT DEFENDANTS' RIGHTS UNDER FISA

As WSJ reported it was going to do, NSA has requested that the FISA Court permit it to retain call data beyond the 5 year age-off date because of all the lawsuits it faces.

> [T]he Government requests that Section (3)E of the Court's Primary Order be amended to authorize the preservation and/or storage of certain call detail records or "telephony metadata" (hereinafter "BR metadata") beyond five years (60 months) after its initial collection under strict conditions and for the limited purpose of allowing the Government to comply with its preservation obligations, described below, arising as a result of the filing of several civil lawsuits challenging the legality of the National Security Agency (NSA) Section 215 bulk telephony metadata collection program.

It provides this introduction to a list of the suits in question.

> The following matters, currently pending either before a United States District Court, or United States Court of Appeals, are among those in which a challenge to the lawfulness of the Section 215 program have been raised:

And lists:

- ACLU v. Clapper

- Klayman v. Obama
- Smith v. Obama, an Idaho case
- First Unitarian Church of LA, the EFF related case
- Paul v. Obama
- Perez v. Clapper, a Bivens suit out of West Texas I hadn't known about before

It goes on to say,

> The duty to preserve typically arises from the common-law duty to avoid spoilation of relevant evidence for use at trial;
>
> [snip]
>
> A party may be exposed to a range of sanctions not only for violating a preservation order,3 but also for failing to produce relevant evidence when ordered to do so because it destroyed information that it had a duty to preserve.
>
> 3 To date, no District Court or Court of Appeals has entered a specific preservation order in any of the civil lawsuits referenced in paragraph 4 but a party's duty to preserve arises apart from any specific court order.
>
> [snip]
>
> When preservation of information is required, the duty to preserve supersedes statutory or regulatory requirements or records-management policies that would otherwise result in the destruction of the information.
>
> [snip]
>
> Based upon the claims raised and the relief sought, a more limited retention

> of the BR metadata is not possible as there is no way for the Government to know in advance and then segregate and retain only that BR metadata specifically relevant to the identified lawsuits.
>
> [snip]
>
> Congress did not intend FISA or the minimization procedures adopted pursuant to section 1801(h) to abrogate the rights afforded to defendants in criminal proceedings.4 For example, in discussing section 1806, Congress stated,
>
> > [a]t the outset, the committee recognizes that nothing in these subsections abrogates the rights afforded a criminal defendant under *Brady v. Maryland*, and the Jencks Act. These legal principles inhere in any such proceeding and are wholly consistent with the procedures detailed here.
>
> [snip]
>
> Although the legislative history discussed above focuses on the use of evidence against a person in criminal proceedings, the Government respectfully submits that the preservation of evidence in civil proceedings is likewise consistent with FISA.
>
> 4 By extension, this should also apply to section 1861(g) which, with respect to retention is entirely consistent with section 1801(h).

Now, if you're not already peeing your pants in laughter, consider the following.

First, as EFF's Cindy Cohn pointed out to the WSJ, Judge Vaughn Walker issued a retention

order in EFF's 2008 suit against the dragnet.

> Ms. Cohn also questioned why the government was only now considering this move, even though the EFF filed a lawsuit over NSA data collection in 2008.
>
> In that case, a judge ordered evidence preserved related to claims brought by AT&T customers. What the government is considering now is far broader.

So, at least in her interpretation, it should already be retaining it.

Then, consider DOJ's very serious citation of Congress' intention that FISA not impair any defendant's criminal rights. It basically says that that principle, laid out during debates about traditional FISA in 1978, should apply to other parts of FISA like the phone dragnet.

Of course, it was only 24 hours ago when DOJ was last caught violating that principle in Section 702, abrogating a defendant's right to know where the evidence against him came from. And there are a whole slew of criminal defendants — most now imprisoned — whose 702 notice DOJ is still sitting on, whose rights DOJ felt perfectly entitled to similarly abrogate (we know this because back in June FBI was bragging about how many of them there were). So I am … surprised to hear DOJ suggest it gives a goddamn about criminal defendants' rights, because for at least the last 7 years it has been shirking precisely that duty as it pertains to FISA.

Also, did you notice what pending case pertaining to the legality of the phone dragnet DOJ didn't mention? Basaaly Moalin's appeal of his conviction based off evidence collected pursuant to Section 215. What do you want to bet that NSA hasn't retained the original phone records that busted him, which would have aged off NSA's servers back in October 2012, well before DOJ told Moalin it had used Section 215 to nab him. That's relevant because, according

to recent reporting, NSA should not have been able to find Moalin's call records given claims about limits on collection; if they did, they probably only did because AT&T was turning over other providers phone records. Moreover, we know that NSA was in violation of the dragnet minimization requirements in a slew of different ways at the time. Notably, that includes queries using selectors that had not been RAS-approved, as required, and dissemination using EO 12333's weaker dissemination rules. Now that we know of these problems, a court might need that original data to determine whether the search that netted Moalin was proper (I presume NSA has the original query results and finished intelligence reports on it, but it's not clear that would explain precisely how NSA obtained that data). Significantly, it was not until after 2009 that NSA even marked incoming data to show where it had been obtained.

So show us (or rather, Moalin's lawyers) the data, NSA.

Ah well. If nothing else, this laughable motion should prove useful for defendants challenging their conviction because DOJ abrogated their rights!

IN SWORN DECLARATION ABOUT DRAGNET, NSA CHANGES ITS TUNE ABOUT SCOPE OF "THIS PROGRAM"

I've been tracking the sudden effort on the part of NSA to minimize how much of the call data in the US it collects (under "this program,"

Section 215).

That effort has, unsurprisingly, carried over to its sworn declarations in lawsuits.

Along with the response in the First Unitarian Church of Los Angeles v. NSA suit the government filed last Friday (this is the EFF-backed suit that challenges the phone dragnet on Freedom of Association as well as other grounds), NSA's Signals Intelligence Director Theresa Shea submitted a new declaration about the scope of the program.

Ostensibly, Shea's declaration serves to explain the "new" "changes" Obama announced last month, which the FISA Court approved on February 4. As I have noted, in one case the "change" simply formalized NSA"s existing practice and in the other it's probably not a big change either.

In addition to her explanation of those "changes," Shea included this language about the scope of the dragnet.

> Although there has been speculation that the NSA, under this program, acquires metadata relating to all telephone calls to, from, or within the United States, that is not the case. The Government has acknowledged that the program is broad in scope and involves the collection and aggregation of a large volume of data from multiple telecommunications service providers, but as the FISC observed in a decision last year, it has never captured information on all (or virtually all) calls made and/or received in the U.S. *See In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR13-109 Amended Mem. Op. at 4 n.5 (F.I.S.C. Aug. 29, 2013) (publicly released, unclassified version) ("The production of all call detail records of all persons in the States has never occurred under under this program.") And

> while the Government has also acknowledged that one provider was the recipient of a now-expired April 23, 2013, Secondary Order from the FISC (Exhibit B to my earlier declaration), the identities of the carriers participating in the program (either now, or at any time in the past) otherwise remain classified. [my emphasis]

Shea appears to be presenting as partial a picture of the dragnet as she did in her prior declaration, where she used expansive language that — if you looked closely — actually referred to the entire dragnet, not just the Section 215 part of it.

Here, she's selectively citing the declassified August 29, 2013 version of Claire Eagan's July 19, 2013 opinion. The latter date is significant, given that the day the government submitted the application tied to that order, NSA General Counsel Raj De made it clear there were 3 providers in the program (see after 18:00 in the third video). These are understood to be AT&T, Sprint, and Verizon.

Shea selectively focuses on language that describes some limits on the dragnet. She could also note that Eagan's opinion quoted language suggesting the dragnet (at least in 2011) collected "substantially all" of the phone records from the providers in question, but she doesn't, perhaps because it would present problems for her "virtually all" claim.

Moreover, Shea's reference to "production of all call detail records" appears to have a different meaning than she suggests it has when read in context. Here's what the actual language of the opinion says.

> Specifically, the government requested Orders from this Court to obtain certain business records of specified telephone service providers. Those telephone

> company business records consist of a very large volume of each company's call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information (CSLI). Primary Ord. at 3 n.l.5
>
> 5 In the event that the government seeks the production of CSLI as part of the bulk production of call detail records in the future, the government would be required to provide notice and briefing to this Court pursuant to FISC Rule 11. The production of all call detail records of all persons in the United States has never occurred under this program. For example, the government [redacted][my emphasis]

In context, the reference discusses not just whether the records of all the calls from all US telecom providers (AT&T, Sprint, and Verizon, which participated in this program on the date Eagan wrote the opinion, but also T-Mobile and Cricket, plus VOIP providers like Microsoft, owner of Skype, which did not) are turned over, but also whether each provider that does participate (AT&T, Sprint, and Verizon) turns over all the records on each call. The passage makes clear they don't do the latter; AT&T, Sprint, and Verizon don't turn over financial data, name, or cell location, for example! And since we know that at the time Eagan wrote this opinion, there were just those 3 providers participating, clearly the records of providers that didn't use the backbone of those 3 providers or, in the case of Skype, would be inaccessible, would be missed. So not all call detail records from the providers that do provide records, nor records covering all the people in the US. But still a "very large volume" from AT&T, Sprint, and Verizon, the providers that happen to be covered by the suit.

And in this declaration, instead of using the number De used last July, Shea instead refers to "multiple telecommunications service providers," which could be 50, 4, 3, or 2, or anywhere in between. Particularly given her "either now, or at any time in the past" language, this suggests the number of providers participating may have changed since July.

Which brings me to the two other implicit caveats in her statement.

First, she suggests (ignoring the time ODNI revealed Verizon's name a second time) that the only thing we can be sure of is that Verizon provided all its domestic data for the 3 months following April 23, 2013.

Actually, we can be fairly sure that at least until January 3, Verizon still participated. That's because the Primary Order approved on that date still includes a paragraph that — thanks to ODNI's earlier redaction fail — we know was written to ensure that Verizon didn't start handing over its foreign call records along with its domestic ones.


B. The Custodian of Records of [redacted]

Though curiously, the way in which DOJ implemented the Obama-directed changes — the ones that Shea's declaration supposedly serves to explain — involved providing substitute language affecting a huge section of the Primary Order, without providing a new Primary Order itself. So we don't know whether ¶1(B) — what I think of as the Verizon paragraph — still exists, or even whether it still existed on February 4, when Reggie Walton approved the change.

Which is particularly interesting given that Shea's declaration just happened to be submitted on the date, February 21, when a significant change in Verizon's structure may have affected how NSA gets its data. (That date was set in

December by a joint scheduling change.)

One way or another, Shea's claim that the dragnet doesn't collect all or even virtually all phone records is very time delimited, certainly allowing the possibility that the scope of the dragnet has changed since the plaintiffs filed this suit on July 16, 3 days before Eagan explicitly excluded cell location data from the dragnet collection, which is the reason NSA's leak recipients now give for limits on the scope of the program.

The claim is also — as claims about the Section 215 always are — very program delimited. In her statement claiming limits on how much data the NSA collects, Shea makes 2 references to "this program" and quotes Eagan making a third. She's not saying the NSA doesn't collect all the phone data in the US (I don't think they quite do that either, but I think they collect more US phone data than they collect under this program). She's saying only that it doesn't collect "virtually all" the phone data in the US "under this program."

Given her previously expansive declaration (which implicitly included all the other dragnet collection methods), I take this declaration as a rather interesting indicator of the limits to the claims about limits to the dragnet.

OBVIOUSLY BOGUS CLAPPER EXONERATION ATTEMPT 5.0 DOESN'T EXACTLY LINE UP WITH OBCEA 4.0

Office of Director of National Intelligence General Counsel Robert Litt, 45 days ago:

> 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.

Director of National Intelligence James Clapper, today:

> But Clapper told The Daily Beast that he simply misunderstood Wyden's question. At the time of the hearing last March, Congress had just finished consideration of a bill to renew the Foreign Intelligence Surveillance Act (FISA). Section 702 of that legislation gives the National Security Agency the authority to collect the electronic communications of non-U.S. persons. In his question, Wyden asked initially if the United States had collected "dossiers" on American citizens and referred to an answer to this question

> by then NSA director, Keith Alexander.
>
> "I was not even thinking of what he was asking about, which is of course we now all know as section 215 of the Patriot Act governing the acquisition and storage of telephony business records metadata," Clapper said. "Wasn't even thinking of that." The director of national intelligence said he thought Wyden's question was actually about section 702 of FISA.
>
> "The allegation about my lying and committing perjury I think are disproven by my labored amplification when I said, 'if there is, it's inadvertent collection,' meaning when we're collecting overseas under section 702, and if we inadvertently collect which we may not know at the time, U.S. persons data, that's what I meant by inadvertent. That comment would make absolutely no sense whatsoever in the context of section 215."
>
> At the time of the Mitchell interview, the U.S. government was still in the process of declassifying elements of the FISA 702 program. "There is only one person on the planet who actually knows what I was thinking," Clapper said of his testimony from last March. "Not the media, and not certain members of Congress, only I know what I was thinking."

If only one person knows what he was thinking, then how was Robert Litt in any position to tell us Clapper was "surprised"?

And has Clapper decided he wasn't "surprised" (perhaps because he had been briefed, not to mention had received months and months of letters, about the question), but instead simply "misunderstood" the intent of a question he had received months of letters about?

SPCMA: THE OTHER NSA DRAGNET SUCKING IN AMERICANS

In December, I wrote a post noting that NSA personnel performing analysis on PATRIOT-authorized metadata (both phone or Internet) can choose to contact chain on just that US-collected data, or — in what's call a "federated query" — on foreign collected data, collected under Executive Order 12333, as well. It also appears (though I'm less certain of this) that analysts can do contact chains that mix phone and Internet data, which presumably is made easier by the rise of smart phones.

Section 215 is just a small part of the dragnet

This is one reason I keep complaining that journalists reporting the claim that NSA only collects 20-30% of US phone data need to specify they're talking about just Section 215 collection. Because we know, in part because Richard Clarke said this explicitly at a Senate Judiciary Committee hearing last month, that Section "215 produces a small percentage of the overall data that's collected." At the very least, the EO 12333 data will include the domestic end of any foreign-to-domestic calls it collects, whether made via land line or cell. And that doesn't account for any metadata

acquired from GCHQ, which might include far more US person data.

The Section 215 phone dragnet is just a small part of a larger largely-integrated global dragnet, and even the records of US person calls and emails in that dragnet may derive from multiple different authorities, in addition to the PATRIOT Act ones.

SPCMA provided NSA a second way to contact chain on US person identifiers

With that background, I want to look at one part of that dragnet: "SPCMA," which stands for "Special Procedures Governing Communications Metadata Analysis," and which (the screen capture above shows) is one way to access the dragnet of US-collected ("1st person") data. SPCMA provides a way for NSA to include US person data in its analysis of foreign-collected intelligence.

According to what is currently in the public record, SPCMA dates to Ken Wainstein and Steven Bradbury's efforts in 2007 to end some limits on NSA's non-PATRIOT authority metadata analysis involving US persons. (They don't call it SPCMA, but the name of their special procedures match the name used in later years; the word, "governing," is for some reason not included in the acronym)

Wainstein and Bradbury were effectively adding a second way to contact chain on US person data.

They were proposing this change 3 years after Collen Kollar-Kotelly permitted the collection and analysis of domestic Internet metadata and 1 year after Malcolm Howard permitted the collection and analysis of domestic phone metadata under PATRIOT authorities, both with some restrictions, By that point, the NSA's FISC-authorized Internet metadata program had already violated — indeed, was still in violation — of Kollar-Kotelly's category restrictions on Internet metadata collection; in fact, the program never came into compliance until it was restarted in 2010.

By treating data as already-collected, SPCMA got around legal problems with Internet metadata

Against that background, Wainstein and Bradbury requested newly confirmed Attorney General Michael Mukasey to approve a change in how NSA treated metadata collected under a range of other authorities (Defense Secretary Bob Gates had already approved the change). They argued the change would serve to make available foreign intelligence information that had been unavailable because of what they described as an "over-identification" of US persons in the data set.

> NSA's present practice is to "stop" when a chain hits a telephone number or address believed to be used by a United States person. NSA believes that it is over-identifying numbers and addresses that belong to United States persons and that modifying its practice to chain through all telephone numbers and addresses, including those reasonably believed to be used by a United States person, will yield valuable foreign intelligence information primarily concerning non-United States persons outside the United States. It is not clear, however, whether NSA's current procedures permit chaining through a United States telephone number, IP address or e-mail address.

They also argued making the change would pave the way for sharing more metadata analysis with CIA and other parts of DOD.

The proposal appears to have aimed to do two things. First, to permit the same kind of contact chaining — including US person data — authorized under the phone and Internet dragnets, but using data collected under other authorities (in 2007, Wainstein and Bradbury said some of the data would be collected under traditional FISA). But also to do so without the dissemination restrictions imposed by FISC on

those PATRIOT-authorized dragnets.

In addition (whether this was one of the goals or not), SPCMA defined metadata in a way that almost certainly permitted contact chaining on metadata not permitted under Kollar-Kotelly's order.

> "Metadata" also means (1) information about the Internet-protocol (IP) address of the computer from which an e-mail or other electronic communication was sent and, depending on the circumstances, the IP address of routers and servers on the Internet that have handled the communication during transmission; (2) the exchange of an IP address and e-mail address that occurs when a user logs into a web-based e-mail service; and (3) for certain logins to web-based e-mail accounts, inbox metadata that is transmitted to the user upon accessing the account.

Some of this information — such as the web-based email exchange — almost certainly would have been excluded from Kollar-Kotelly's permitted categories because it would constitute content, not metadata, to the telecoms collecting it under PATRIOT Authorities.

Wainstein and Bradbury appear to have gotten around that legal problem — which was almost certainly the legal problem behind the 2004 hospital confrontation — by just assuming the data was already collected, giving it a sort of legal virgin birth.

Doing so allowed them to distinguish this data from Pen Register data (ironically, precisely the authority Kollar-Kotelly relied on to authorize PATRIOT-authorized Internet metadata collection) because it was no longer in motion.

> First, for the purpose of these provisions, "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing or

> signaling information." 18 U.S.C. § 3127(3); 50 U.S.C. § 1841 (2). When NSA will conduct the analysis it proposes, however, the dialing and other information will have been already recorded and decoded. Second, a "trap and trace device" is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information." 18 U.S.C. § 3127(4); 50 U.S.C. § 1841(2). Again, those impulses will already have been captured at the point that NSA conducts chaining. Thus, NSA's communications metadata analysis falls outside the coverage of these provisions.

And it allowed them to distinguish it from "electronic surveillance."

> The fourth definition of electronic surveillance involves "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication …. " 50 U.S.C. § 1802(f)(2). "Wire communication" is, in turn, defined as "any communication while it is being carried by a wire, cable, or other like com1ection furnished or operated by any person engaged as a common carrier …. " !d. § 1801 (1). The data that the NSA wishes to analyze already resides in its databases. The proposed analysis thus does not involve the acquisition of a communication "while it is being carried" by a connection furnished or operated by a common carrier.

This legal argument, it seems, provided them a way to carve out metadata analysis under DOD's secret rules on electronic surveillance, distinguishing the treatment of this data from "interception" and "selection."

> For purposes of Procedure 5 of DoD Regulation 5240.1-R and the Classified Annex thereto, contact chaining and other metadata analysis don't qualify as the "interception" or "selection" of communications, nor do they qualify as "us[ing] a selection term," including using a selection term "intended to intercept a communication on the basis of … [some] aspect of the content of the communication."

This approach reversed an earlier interpretation made by then Counsel of DOJ's Office of Intelligence and Policy Review James A Baker.

Baker may play an interesting role in the timing of SPCMA. He had just left in 2007 when Bradbury and Wainstein proposed the change. After a stint in academics, Baker served as Verizon's Assistant General Counsel for National Security (!) until 2009, when he returned to DOJ as an Associate Deputy Attorney General. Baker, incidentally, got named FBI General Counsel last month.

NSA implemented SPCMA as a pilot in 2009 and more broadly in 2011

It wasn't until 2009, amid NSA's long investigation into NSA's phone and Internet dragnet violations that NSA first started rolling out this new contact chaining approach. I've noted that the rollout of this new contact-chaining approach occurred in that time frame.

Comparing the name …

> SIGINT Management Directive 424 ("SIGINT Development-Communications Metadata Analysis") provides guidance on the NSA/CSS implementation of the "Department of Defense Supplemental Procedures Governing Communications Metadata Analysis" (SPCMA), as approved by the U.S. Attorney General and the Secretary of Defense. [my emphasis]

And the description of the change …

> Specifically, these new procedures permit contact chaining, and other analysis, from and through any selector, irrespective of nationality or location, in order to follow or discover valid foreign intelligence targets. (Formerly analysts were required to determine whether or not selectors were associated with US communicants.) [emphasis origina]

,,, Make it clear it is the same program.

NSA appears to have made a few changes in the interim. In 2007, Wainstein and Bradbury said it might include FISA-collected data and "other authorities" (suggesting they might use STELLAR WIND data). In its 2011 rollout, it reportedly applied only to EO 12333 collected data.

In addition, the original proposal focused primarily on contact-chaining. In the implementation, SPCMA permitted "other analysis" as well.

The later (internal to NSA) description also makes it much more clear the point is to identify ties between foreign targets and Americans.

> In the first place it allows NSA to discover and track connections between foreign intelligence targets and possible 2nd Party or US communicants.

Finally, as implemented, SPCMA required analysts to adhere to existing dissemination rules; given that this is EO 12333 data, that still would permit broader dissemination than under the PATRIOT-authorized dragnet, but may not have resulted in as unfettered sharing with the CIA as NSA had wanted.

Additionally, in what would have been true from the start but was made clear in the roll-out, NSA could use this contact chaining for any

foreign intelligence purpose. Unlike the PATRIOT-authorized dragnets, it wasn't limited to al Qaeda and Iranian targets. NSA required only a valid foreign intelligence justification for using this data for analysis.

> The primary new responsibility is the requirement:

- to enter a foreign intelligence (FI) justification for making a query or starting a chain, [emphasis original]

Now, I don't know whether or not NSA rolled out this program because of problems with the phone and Internet dragnets. But one source of the phone dragnet problems, at least, is that NSA integrated the PATRIOT-collected data with the EO 12333 collected data and applied the protections for the latter authorities to both (particularly with regards to dissemination). NSA basically just dumped the PATRIOT-authorized data in with EO 12333 data and treated it as such. Rolling out SPCMA would allow NSA to use US person data in a dragnet that met the less-restrictive minimization procedures.

But, as I said, at least until late 2011, from when the screen caption above was taken, SPCMA metadata analysis was available from the very same interface as PATRIOT-authority analysis (as well as "normal," which may be EO 12333 data excluding US person identifiers). As I've noted in the past, that same training program coached analysts how to re-run PATRIOT-authority queries to obtain EO 12333 results that could be more broadly shared.

That "other analysis" permitted under SPCMA

I'm really just beginning to understand SPCMA and how it works. I certainly have no idea how broadly NSA collects the EO 12333 data that gets dumped into it, and to what degree it replicates

domestically collected data. At best, it could only include data that companies like Verizon made available off shore, but it would also include a lot of data not collected under the PATRIOT authorities.

But, especially given discussions lately about difficulties NSA has integrating cell data because of geolocation information, I'm particularly interested that one of NSA's pilot co-traveler programs, CHALKFUN, works with SPCMA.

> Chalkfun's Co-Travel analytic computes the date, time, and network location of a mobile phone over a given time period, and then looks for other mobile phones that were seen in the same network locations around a one hour time window. When a selector was seen at the same location (e.g., VLR) during the time window, the algorithm will reduce processing time by choosing a few events to match over the time period. Chalkfun is SPCMA enabled1.

> 1 (S//SI//REL) SPCMA enables the analytic to chain "from," "through," or "to" communications metadata fields without regard to the nationality or location of the communicants, and users may view those same communications metadata fields in an unmasked form. [my emphasis]

Now, aside from what this says about the dragnet database generally (because this makes it clear there is location data in the EO 12333 data available under SPCMA, though that was already clear), it makes it clear there is a way to geolocate US persons — because the entire point of SPCMA is to be able to analyze data including US persons, without even any limits on their location (meaning they could be in the US).

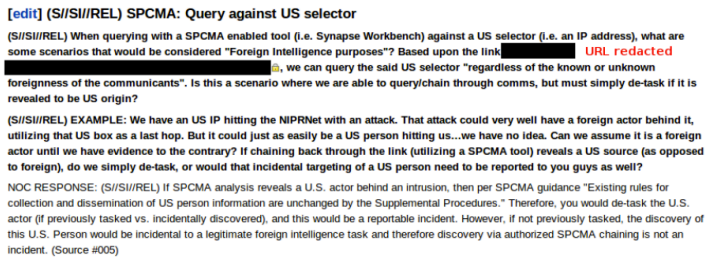
I think it marginally possible NSA might be

forced to deactivate such functions if it is forced to do so domestically more generally. But at least in October 2012 (so long after *US v. Jones*), it appears NSA permitted geolocation of US persons within the US using CHALKFUN under SPCMA.

Again, I'm just beginning to understand how SPCMA has been enacted. But it seems to provide a nice big loophole to analyze US person metadata under guidelines that are far more permissive than the PATRIOT-authorized authorities. Including, at least until 2012, geolocation. There's a lot of data that won't be available under this program (and NSA has to claim it is aiming to collect non-US data under EO 12333).

But what data it does get collected … "incidentally" … gets exposed to far more analysis than that under the PATRIOT authorized dragnets.

Update: This passage, from documents released in Glenn Greenwald's latest, shows how SPCMA still requires queries to target a foreign entity (though you can see how they coach using a foreign tasker so as to permit the chaining).



[edit] (S//SI//REL) SPCMA: Query against US selector

(S//SI//REL) When querying with a SPCMA enabled tool (i.e. Synapse Workbench) against a US selector (i.e. an IP address), what are some scenarios that would be considered "Foreign Intelligence purposes"? Based upon the link [redacted] URL redacted [redacted], we can query the said US selector "regardless of the known or unknown foreignness of the communicants". Is this a scenario where we are able to query/chain through comms, but must simply de-task if it is revealed to be US origin?

(S//SI//REL) EXAMPLE: We have an US IP hitting the NIPRNet with an attack. That attack could very well have a foreign actor behind it, utilizing that US box as a last hop. But it could just as easily be a US person hitting us…we have no idea. Can we assume it is a foreign actor until we have evidence to the contrary? If chaining back through the link (utilizing a SPCMA tool) reveals a US source (as opposed to foreign), do we simply de-task, or would that incidental targeting of a US person need to be reported to you guys as well?

NOC RESPONSE: (S//SI//REL) If SPCMA analysis reveals a U.S. actor behind an intrusion, then per SPCMA guidance "Existing rules for collection and dissemination of US person information are unchanged by the Supplemental Procedures." Therefore, you would de-task the U.S. actor (if previously tasked vs. incidentally discovered), and this would be a reportable incident. However, if not previously tasked, the discovery of this U.S. Person would be incidental to a legitimate foreign intelligence task and therefore discovery via authorized SPCMA chaining is not an incident. (Source #005)

KEITH ALEXANDER REFUTES CLAIMS NSA DOESN'T GET CELL DATA

Eight days ago, the country's four major

newspapers reported a claim that the NSA collected 33% or less of US phone records (under the Section 215 program, they should have specified, but did not) because it couldn't collect most cell phone metadata:

- "[I]t doesn't cover records for most cellphones," (WSJ)
- "[T]he agency has struggled to prepare its database to handle vast amounts of cellphone data," (WaPo)
- "[I]t has struggled to take in cellphone data," (NYT)
- "[T]he NSA is gathering toll records from most domestic land line calls, but is incapable of collecting those from most cellphone or Internet calls." (LAT)

Since that time, I have pointed to a number of pieces of evidence that suggest these claims are only narrowly true:

- A WSJ article from June made it clear the cell gap, such as it existed, existed primarily for Verizon and T-Mobile, but their calls were collected via other means (the WaPo and NYT both noted this in their stories without considering how WSJ's earlier claim it was still near-comprehensive contradicted the 33% claim)
- The NSA's claimed Section 215 dragnet successes — Basaaly Moalin, Najibullah

Zazi, Tsarnaev brothers — all involved cell users

- Identifying Moalin via the dragnet likely would have been impossible if NSA didn't have access to T-Mobile cell data
- The phone dragnet orders specifically included cell phone identifiers starting in 2008
- Also since 2008, phone dragnet orders seem to explicitly allow contact-chaining on cell identifiers, and several of the tools they use with phone dragnet data specifically pertain to cell phones

Now you don't have to take my word for it. Here's what Keith Alexander had to say about the claim Friday:

> Responding to a question about recent reports that the NSA collects data on only 20% to 30% of calls involving U.S. numbers, Alexander acknowledged that the agency doesn't have full coverage of those calls. He wouldn't say what fraction of the calls NSA gets information on, but specifically denied that the agency is completely missing data on calls made with cell phones.
>
> "That part is not true," he said. "We don't get it all. We don't get 100% of the data. It's not where we want it to be, but it has been sufficient to go after the key targets that we're going after." [my emphasis]

Admittedly, Alexander is not always entirely honest, so it's possible he's just trying to dissuade terrorists from using cellphones while the NSA isn't tracking them. But he points to the same evidence I did — that NSA has gotten key targets who use cell phones.

There's something else Alexander said that might better explain the slew of claims that it can't collect cell phone data.

> The NSA director, who is expected to retire within weeks, indicated that some of the gaps in coverage are due to the fact that the NSA "paused any changes to the program" during the recent controversy and discussions about restructuring the effort.

The NSA has paused changes to the program.

This echoes WaPo and WSJ reports that crises (they cited both the 2009 and current crisis) delayed some work on integrating cell data, but suggests that NSA was already making changes when the Snowden leaks started.

There is evidence the pause — or at least part of it — extends back to before the Snowden leak. As I reported last week, even though the NSA has had authority to conduct a new auto-alert on the phone dragnet since November 2012, they've never been able to use it because of technical reasons.

> The Court understands that to date NSA has not implemented, and for the duration of this authorization will not as a technical matter be in a position to implement, the automated query process authorized by prior orders of this Court for analytical purposes.

This description actually came from DOJ, not the FISC, and I suspect the issue is rather that NSA has not solved some technical issues that would allow it to perform the auto-alert within the

legal limits laid out by the FISC (we don't know what those limits are because the Administration is withholding the Primary Order Supplement that would describe it, and redacting the description of the search itself in all subsequent orders).

That said, there are plenty of reasons to believe there are new reasons why NSA is having problems collecting cell phone data because it includes cell location, which is far different than claiming (abundant evidence to the contrary) they haven't been collecting cell data all this time. In addition to whatever reason NSA decided to stop its cell location pilot in 2011 and the evolving understanding of how the *US v. Jones* decision might affect NSA's phone dragnet program, 3 more things have happened since the beginning of the Snowden leaks:

- On July 19, Claire Eagan specifically excluded the collection of cell site location information under the Section 215 authority
- On September 1, NYT exposed AT&T's Hemisphere program; not only might this give AT&T reason to stop collating such data, but if Hemisphere is the underlying source for AT&T's Section 215 response, then it includes cell location data that is now prohibited
- On September 2, Verizon announced plans to split from Vodaphone, which might affect how much of its data, including phone metadata, is available to NSA via GCHQ under the Tempora program;

> that change legally takes effect February 21

Remember, too, there's a February 2013 FISC Section 215 opinion the Administration is also still withholding, which also might explain some of the "technical-meaning-legal" problems they're having.

Underlying this all (and assuredly underlying the problems with collecting VOIP calls, which are far easier to understand and has been mentioned in some of this reporting, including the LAT story) is a restriction arising from using an ill-suited law like Section 215 to collect a phone dragnet: telecoms can only be obligated to turn over records they actually "already generate," as described by NSA's SID Director Theresa Shea.

> [P]ursuant to the FISC's orders, telecommunications service providers turn over to the NSA business records that the companies already generate and maintain for their own pre-existing business purposes (such as billing and fraud prevention).

To the extent telecoms use SS7 data, which includes cell location, to fulfill their Section 215 obligation (after all, what telecoms need billing records on a daily basis?), it probably does introduce problems.

Which, I suspect, will mean that Alexander and the rest of the dragnet defenders will recommend that a third party collate and store all this data, the worst of all solutions. They need to have a comprehensive source (like Hemisphere apparently plays for the DEA), one that will shield the government from necessarily having collected cell location data that is increasingly legally suspect to obtain. And they'll celebrate it as a great sop to the civil libertarians, too, when in fact, they've probably reached the point where it is clear Section 215 can't legally authorize what it is

they want it to do.

The issue, more and more evidence suggests, is that they can’t collect the dragnet data without a law designed to construct the dragnet. Which is another way of saying the dragnet, as intended to function, is illegal.