DOJ'S MULTIPLE AUTHORITIES FOR DESTROYING EVIDENCE

It seems like aeons ago, but just a week ago, EFF and DOJ had a court hearing over preserving evidence in the EFF lawsuits (Shubert, Jewel, and First Unitarian Church v. NSA). As I noted in two posts, a week ago Monday DOJ surprised EFF with the news that it had been following its own preservation plan, which it had submitted ex parte to Vaughn Walker, rather than the order Walker subsequently imposed. As a result, it has been aging off data in those programs (notably the PATRIOT-authorized Internet and phone dragnets) authorized by law, as opposed to what it termed Presidential authorization. DOJ's behavior makes it clear that it is trying to justify treating some data differently by claiming it was collected under different authorities.

Remember, there are at least five different legal regimes involved in the metadata dragnet:

- EO 12333 authority for data going back to at least 1998
- Stellar Wind authority lasting until 2004, 2006, and 2007 for different practices
- PATRIOT-authorized authorities for Internet (until 2011) and phone records (until RuppRoge or something else passes)
- SPCMA, which is a subset of EO 12333 authority that conducts potentially problematic contact chaining integrating US person

Internet metadata
- Five Eyes, which is EO 12333, but may involve GCHQ equities or, especially, ownership of the data

At the hearing and in their motions, EFF argued that their existing suits are not limited to any particular program (they didn't name all these authorities, but they could have). Rather, they are about the act of dragnetting, regardless of what authority (so they'll still be live suits after RuppRoge passes, for example).

EFF appears to have at least partly convinced Judge Jeffrey White, because on Friday he largely sided with EFF, extending the preservation order and — best as I can tell — endorsing EFF's argument that their suits cover the act of dragnetting, rather than just the Stellar Wind, FISA Amendments Act, or phone and Internet dragnets.

With that as background, I want to look at a few things from the transcript of last Wednesday's hearing. First, at one point White suggested there might be a — purely hypothetical, mind you — event that happened 5 years ago the plaintiffs might need live data from.

> THE COURT: Well, what if the NSA was doing something, say, five years ago that was broader in scope, and more problematical from the constitutional perspective, and those documents are now aged out? And — because now under the FISC or the orders of the FISC Court, the activities of the NSA have — I mean, again, this is all hypothetical — have narrowed. And wouldn't the Government — wouldn't the plaintiffs then be deprived of that evidence, if it existed, of a broader, maybe

> more constitutionally problematic evidence, if you will?
>
> MR. GILLIGAN: There – we submit a twofold answer to that, Your Honor.
>
> We submit that there are documents that – and this goes to Your Honor's Question 5B, perhaps. There are documents that could shed light on the Plaintiffs' standing, whether we've actually collected information about their communications, even in the absence of those data.
>
> As far as – as Your Honor's hypothetical goes, it's a question that I am very hesitant to discuss on the public record; but I can say if this is something that the Court wishes to explore, we could we could make a further classified ex parte submission to Your Honor on that point.

Of course, this is not at all hypothetical. By NSA's own admission, they were watchlisting 3,000 US persons until just over 5 years ago without the requisite First Amendment review. And Theresa Shea has submitted another sealed filing in the suit, so White may know that. (Or maybe he reads yours truly – I believe I still am the only person to have reported this, though it is in public records). Now, White doesn't hint at this, but this concern would already implicate two authorities, because the US persons were watchlisted under EO 12333 authorities (possibly SPCMA), dumped into Section 215 data, then moved back onto the EO 12333 lists.

Then there are a few ridiculous, more general claims. DOJ claimed it would take the most advanced SIGINT Agency in the world "many months" and hours of personnel time and technological resources to figure out how to save data onto a storage medium.

> Because we're talking about a periodic transition of data from the operational database to a preservation medium, we've got to develop a capability to do that, which is going to require a software-development effort that could take many months, and involve a diversion of many NSA resources.

EFF's Cindy Cohn noted, these claims of hardship are particularly odd given that the NSA proposed keeping all the data before the FISA Court.

> I'm a little confused about why they're fighting in front of you for the very thing they asked for in the FISC. They didn't talk about operational problems or difficulties preserving it when they asked the FISC for permission for this on March 7.

Judge White not only mocked this in the hearing, he basically extended the preservation order.

> MR. GILLIGAN: I think the answer to this question, Your Honor, brings us back to the discussion we were having with respect to your first question. The — migrating the data to tape would require, because we're dealing here with a live program, where data are coming in and data are periodically being aged off, rather than a program that has been terminated, and you have a static data set, you're going to have to or the NSA is going to have to engage in a complicated software-development effort to basically come up with a capability of periodically aging data off from the

> operational database into a preservation medium.
>
> THE COURT: But you're not saying the NSA, with all of its computer expertise, can't do this. You're not saying it's impossible to do it. You're saying it would be a burden financially and perhaps operationally, but it can be done; can it not?
>
> MR. GILLIGAN: Your Honor, we have not said it can't be done. If it – but again, it would be at significant costs that are detailed in classified declaration, and would result in a diversion of financial, technological, and personnel resources from the NSA's core national-security mission.

Then DOJ argued – in a lawsuit brought, in part, because the government has utterly blown up the definition of relevant – that relevance must be defined very narrowly here.

> Is this relevant evidence that is so potentially beneficial to the Plaintiffs' case, that preservation is required, notwithstanding the burden of doing so?
>
> We – we – simply ascertaining that the data are relevant within the meaning of the Rule 26 is only the start of the inquiry. It's not – it doesn't get us the answer to the question.

On both of these, you see how the multiple authorities involved could make the issue more difficult. EO 12333 data may not have age off dates, 215 query **results** definitely don't, and GCHQ won't want to do anything with their data because our government is being sued. And one way to make all of this easier is to define relevance to those programs that FISC has authority over.

I'm most interested in the following exchange:

> This Court's jurisdiction is to determine what our preservation obligation is; but apart from preserving data, **what access we should have to it is something that should be determined by the FISC, and in accordance with statutes and regulations and Executives Orders that otherwise govern such matters**.
>
> THE COURT: On minimization?
>
> MR. GILLIGAN: On minimization, yes. Principally, minimization; **but perhaps otherwise**. The other thing that troubles us in this language is that I could foresee, particularly after the debate we've been having today, all in good faith, that we could find ourselves here three or four years down the road, arguing whether or not this language imposed some sort of independent restriction on the Government's access to preserve[d] data, which it absolutely should not do. Why – the Court's writ here is to tell us whether or not to preserve; **but what access we should have to our own data while it's being preserved is something, again, that is not at issue in this litigation**.
>
> [snip]
>
> MR. GILLIGAN: It would – within – any access we should have to that aged-out data would have to be with the permission of the FISC, and in accordance with FISC orders. The language here, Your Honor, I don't believe accomplishes the objective that Ms. Cohn just described. I'm either misunderstanding the language, or I'm misunderstanding Ms. Cohn's explanation of it. It says nothing in this order – this is language that Plaintiffs would have this Court enter – nothing in this

> order where the Court's prior preservation orders shall be construed as authorizing any review or use of telephone orders records or intelligence gathering for any other nonlitigation purposes. What we fear is that this — **we don't want sort of a day to come where there's an argument that this language independently barred us from accessing the data**. Any restrictions on our access to the data are — should be imposed by the FISC in accordance with the terms of FISA. To the extent that that —
>
> THE COURT: So it's a jurisdictional issue, is really what you're saying?
>
> MR. GILLIGAN: Right. The Congress, through FISA, conferred on the FISC the authority to determine whether and under what circumstances the particular personnel should have access to data that are acquired under the authority of FISA.

The same DOJ that has agreed in FISC to not touch any data archived for this preservation order is here saying that White can't impose any such order because it's their data damnit and they can access it if they want to!

It's a seeming contradiction.

Except it's not, not even for the Section 215 data, because the data in question may well be in the corporate store! That data would be the most important to show the plaintiffs' exposure.

Moreover, there's all the other data — the 12333, the SPCMA, GCHQ's own data — that they have limited restrictions on accessing, each having also fed the corporate store.

But here's the thing: The government got White not to impose this protection order here based on a claim that it falls under FISC's jurisdiction. And that's true for the small fraction of it that derives from Section 215.

But the bulk of it doesn't arise from 215, it arises from 12333.

Which is, in part, what Gilligan was referring to when he raised "statutes and regulations and Executives Orders." Except that for that data, White should be entitled to jurisdiction because FISA doesn't.

Meanwhile, DOJ wants to delete the legally collected stuff and keep playing with the rest of it.

RUPPROGE FAKE DRAGNET FIX REQUIRES INTEL COMMUNITY TO UPDATE 30 YEAR OLD EO 12333 PROCEDURES

One good aspect of the RuppRoge Fake Dragnet Fix is its measure requiring all elements of the Intelligence Community to comply with the EO that governs them.

At issue is this clause in EO 12333 requiring that any element of the Intelligence Community collecting data on US persons have Attorney General approved procedures for handling that data.

> 2.3 Collection of information. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with

> the authorities provided by Part 1 of this Order, after consultation with the Director.

This is something PCLOB asked Eric Holder and James Clapper to make sure got done back in August. In their letter, they disclosed some agencies in the IC have been stalling on these updates almost 3 decades.

> The Privacy and Civil Liberties Oversight Board just sent a letter to Eric Holder and James Clapper requesting that they have all the Intelligence Committee agencies update what are minimization procedures (though the letter doesn't call them that), "to take into account new developments including technological developments."
>
> > As you know, Executive Order 12333 establishes the overall framework for the conduct of intelligence activities by U.S. intelligence agencies. Under section 2.3 of the Executive Order, intelligence agencies can only collect, retain, and disseminate information about U.S. persons if the information fits within one of the enumerated categories under the Order and if it is permitted under that agency's implementing guidelines approved by the Attorney General after consultation with the Director of National Intelligence.
> >
> > The Privacy and Civil Liberties Oversight Board has learned that **key procedures that form the guidelines to protect "information concerning United States person" have not comprehensively been updated, in some cases in almost three**

> > **decades**, despite dramatic changes in information use and technology. [my update]

In other words, these procedures haven't been updated, in some cases, since not long after Ronald Reagan issued this EO in 1981.

RuppRoge aims to require the IC elements to comply.

> (1) REQUIREMENT FOR IMMEDIATE REVIEW.—Each head of an element of the intelligence community that has not obtained the approval of the Attorney General for the procedures, in their entirety, required by section 2.3 of Executive Order 12333 (50 U.S.C. 3001 note) within 5 years prior to the data of the enactment of the End Bulk Collection Act of 2014, shall initiate, not later than 180 days after such enactment, a review of the procedures for such element.

Mind you, asking agencies to **initiate** a review 6 months after passage of a bill to update procedures that are 30 years old isn't exactly lighting a fire under IC arse. But then, the delay probably stems from some agencies hoarding agency records on US persons that are even older than the EO.

NSA BIDS TO EXPAND SPYING IN GUISE OF "FIXING" PHONE

DRAGNET

Dutch Ruppersberger has provided Siobhan Gorman with details of his plan to "fix" the dragnet — including repeating the laughable claim that the "dragnet" (which she again doesn't distinguish as solely the Section 215 data that makes up a small part of the larger dragnet) doesn't include cell data.

Only, predictably, it's not a "fix" of the phone dragnet at all, except insofar as NSA appears to be bidding to use it to do all the things they want to do with domestic dragnets but haven't been able to do legally. Rather, it appears to be an attempt to outsource to telecoms some of the things the NSA hasn't been able to do legally since 2009.

For example, there's the alert system that Reggie Walton shut down in 2009.

As I reported back in February, the NSA reportedly has never succeeded in replacing that alert system, either for technical or legal reasons or both.

> NSA reportedly can't get its automated chaining program to work. In the motion to amend, footnote 12 — which modifies part of some entirely redacted paragraphs describing its new automated alert approved back in 2012 — reads:
>
> > 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. Accordingly, this amendment to the Primary Order authorizes the use of this automated query process for development and testing purposes

> > only. No query results from such testing shall be made available for analytic purposes. Use of this automated query process for analytical purposes requires further order of this Court.
>
> PCLOB describes this automated alert this way.
>
> > In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to process its calling records.68 The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store."
>
> It has been 15 months since FISC approved this alert, but NSA still can't get it working.
>
> I suspect this is the root of the stories claiming NSA can only access 30% of US phone records.

As described by WSJ, this automated system will be built into the orders NSA provides telecoms; once a selector has been provided to the telecoms, they will keep automatically alerting on it.

> > Under the new bill, a phone company

> would search its databases for a phone number under an individual "directive" it would receive from the government. It would send the NSA a list of numbers called from that phone number, and possibly lists of phone numbers those numbers had called. **A directive also could order a phone company to search its database for such calls as future records come in**. [my emphasis]

This would, presumably, mean NSA still ends up with a corporate store, a collection of people against whom the NSA has absolutely not a shred of non-contact evidence, against whom they can use all their analytical toys, including searching of content.

Note, too, that this program uses the word "directive," not query. Directive comes from the PRISM program, where the NSA gives providers generalized descriptions and from there have broad leeway to add new selectors. Until I hear differently, I'll assume the same is true here: that this actually involves less individualized review before engaging in 2 degrees of Osama bin Laden.

The legislation seems ripe for inclusion of querying of Internet data (another area where the NSA could never do what it wanted to legally after 2009), given that it ties this program to "banning" (US collection of, but Gorman doesn't say that either, maintaining her consistency in totally ignoring that EO 12333 collection makes up the greater part of bulk programs) Internet bulk data collection.

> The bill from Intelligence Committee Chairman Mike Rogers (R., Mich.) and his Democratic counterpart, Rep. C.A. "Dutch" Ruppersberger (D., Md.), would ban so-called bulk collection of phone, email and **Internet** records by the government, according to congressional aides familiar with the negotiations. [my emphasis]

Call me crazy, but I'm betting there's a way they'll spin this to add in Internet chaining with this "fix."

Note, too, Gorman makes no mention of location data, in spite of having tied that to her claims that NSA only collects 20% of data. Particularly given that AT&T's Hemisphere program provides location data, we should assume this program could too, which would present a very broad expansion on the status quo.

And finally, note that neither the passage I quoted above on directives to providers, nor this passage specifies what kind of investigations this would be tied to (though they are honest that they want to do away with the fig leaf of this being tied to investigations at all).

> The House intelligence committee bill doesn't require a request be part of an ongoing investigation, Mr. Ruppersberger said, because intelligence probes aim to uncover what should be investigated, not what already is under investigation.

Again, the word "directive" in the PRISM context also provides the government the ability to secretly pass new areas of queries — having expanded at least from counterterrorism to counterproliferation and cybersecurity uses. So absent some very restrictive language, I would assume that's what would happen here: NSA would pass it in the name of terrorism, but then use it primarily for cybersecurity and counterintelligence, which the NSA considers bigger threats these days.

And that last suspicion? That's precisely what Keith Alexander said he planned to do with this "fix," presumably during the period when he was crafting this "fix" with NSA's local Congressman: throw civil libertarians a sop but getting instead an expansion of his cybersecurity authorities.

Update: Here's Spencer on HPSCI, confirming it's

as shitty as I expected.

And here's Charlie Savage on Obama's alternative.

It would:

- Keep Section 215 in place, though perhaps with limits on whether it can be used in this narrow application
- Enact the same alert-based system and feed into the corporate store, just as the HPSCI proposal would
- Include judicial review like they have now (presumably including automatic approval for FISA targets)

Obama's is far better than HPSCI (though this seems to be part of a bad cop-good cop plan, and the devil remains in the details). But there are still some very serious concerns.

THE OCTOBER 30, 2009 STATEMENT OF AUTHORITIES: THE EFF DOCUMENT FIGHT COULD GET VERY INTERESTING

If the Chief FISC Judge accuses the government of material misrepresentations but no one but a dirty fucking hippie blogger reports it, did it happen?

On Friday, I reported on Judge Reggie Walton's cranky opinion asking for an explanation about why the government didn't tell him EFF believed they had a protection order in cases relevant to the dragnets. And while it overstates the resounding silence to say that only your esteemed DFH host reported it — TechDirt had a good report — some of the other reporting on it thus far seems to have missed the whole material misrepresentation judgement in Walton's order.

But I think it's not yet clear — to anyone — how interesting this document fight could get.

Just as one example of why (I'll develop some of the others over the next couple of days, I hope), consider the October 30, 2009 statement of authorities.

Earlier this month, I noted that EFF had submitted a list of filings that the government had not released in spite of what they believed to be Judge Jeffrey White's order to declassify everything.

- April 9, 2007 notices indicating FISC Judge rejected early bulk orders
- October 25, 2007 government challenge to motion to protect evidence, with ex parte NSA official declaration submitted in Shubert
- April 3, 2009 supplemental memorandum in Jewel
- October 30, 2009 supplemental memorandum on points of authority in Shubert
- November 2012

In last Wednesday's hearing, the government claimed they didn't have to release these

because they engaged in a colloquy limiting White's orders to the state secrets declarations. And for the moment, I'll take that as accurate.

But since then, the government has released one of these — the October 25, 2007 challenge to the protection motion — as part of their filing on Monday fighting a protection order in EFF's phone dragnet suit. And that document was pretty stunning. Not only did it show the government had redefined the Multidistrict Litigation suits so as to exclude any of the FISA-authorized metadata dragnets that EFF of course had no way of knowing about yet. But in the filing, the government revealed that because of this filing and in defiance of Vaughn Walker's November 2007 protection order, it has been destroying the metadata dragnet data in the interim.

In other words, the government is withholding these filings because they're fairly damning.

Which got me thinking about the timing and significance of the October 30, 2009 supplemental memorandum on points of authority supporting a motion to dismiss the Shubert suit based on sovereign immunity and state secrets.

At one level, the memorandum is not all that suspicious. As you can see above, the government filed what is presumably roughly the same filing at the analogous time in Jewel, just as it was making its state secrets bid.

But I find the timing of the October 30 filings in Shubert to be of particular interest. That's because a 2011 NSA training program seems to indicate that the Internet dragnet shut down at almost precisely that time, as it indicates that Internet dragnet data collected prior to November 2009 requires some sort of special treatment.

> In addition, in the source information at the end of the line, the SIGAD [redacted] BR data can be recognized by SIGADs beginning with [redacted] For PR/TT, data collected after October 2010

> is found [redacted] For a comprehensive listing of all the BR and PR/TT SIGADs as well as information on **PR/TT data collected prior to November of 2009**, contact your organization's management or subject matter expert.

Remember, Shubert was suing for illegal wiretapping. And while Judge John Bates did not fully assess what NSA was doing — which appears to be collecting data that counts as content in the guise of collecting metadata — until the following year (some time between July and October 2010), when he did so, he implied the government had to comply with the laws in which they were claiming, in 2009, they had sovereign immunity. And the government **had to know** by that point they had serious legal problems with the Internet dragnet.

Indeed, the government kept asking for extensions leading up to this filing — at the time they claimed it was because of DOJ's whats-old-is-new state secrets policy. Altogether they got an extra 22 days to file this filing (which should have been substantially similar to the ones they filed in April). They were almost certainly having still-undisclosed problems with the phone dragnet (probably relating to dissemination of data), as the October 30, 2009 phone dragnet orders is one of the ones the government has withheld even though it is obviously responsive to ACLU and EFF's FOIA. But the discussions on the Internet dragnet must have been even more contentious, given that the FISC (probably either Reggie Walton or John Bates) refused to reauthorize it. (Note, October 30, 2009 was a Friday, so if FISC formally didn't approve the Internet dragnet in October 2009, it would have been that day).

And the thing is, from Keith Alexander's state secrets declaration, submitted perhaps hours and almost certainly no more than a month before the Internet dragnet got shut down because it was illegally collecting metadata that was legally content, it's not at all clear that the

government fully disclosed details they knew about those legal problems with the dragnet. Look closely at ¶¶ 27 and 28, ¶¶48-56, ¶¶58-62 with footnotes.

The phone dragnet description hides the problems with ongoing dissemination problems (which the Administration hid from Congress, as well). It also makes no mention that the phone dragnet had US persons on an alert list without reviewing those selectors for First Amendment review, something that should be central to the suits against NSA (see in particular ¶60). And while there are redacted sentences and footnotes — 13 and 24 — which could include notice that the government was (and had been, since the inception of the FISC-authorized Internet dragnet) collecting metadata that counted as content, those are all very brief descriptions. Moreover, the unredacted descriptions clearly claim that the Internet dragnet program collects no content, which legally it almost certainly did. Moreover, note that the references to the Internet dragnet speak of it in the present tense: "Pursuant to the FISA Pen Register, …. NSA is authorized to collect in bulk."But there doesn't seem to be the parallel structure in ¶28 where you'd expect the government to confess that the program was imminently shutting down because it was illegally collecting Internet content.

Note, too, how the declaration refers to the reauthorizations. ¶59 describes the phone dragnet authority "continuing until October 30, 2009" and ¶58 describes the Internet dragnet "requires continued assistance by the providers through [redacted] 2009. They appear not to have known for sure whether the programs would be reauthorized **that night**! But they appear not to have explained why not.

Perhaps the most pregnant paragraph is ¶62, which in context appears to relate only to the phone dragnet, though I suspect the government would point to to claim their description of violations was not comprehensive:

> NSA is committed to working with the FISC on this **and other compliance issues** to ensure that this vital intelligence tool works appropriately and effectively. For purposes of this litigation, and the privilege assertions now made by the DNI and by the NSA, the intelligence sources and methods described herein remain highly classified and the disclosure that [redacted] would compromise vital NSA sources and methods and result in exceptionally grave harm to national security.

By any measure, Alexander's declaration falls short of what the government already knew at that time, demonstrably so in the case of the phone dragnet. He hid details — significantly, the watchlist of Americans that violated statute, and almost certainly that the NSA was collecting content in the name of metadata — that were material to the suits at hand.

Which brings me to the memo on authorities. Even as the government was hiding material violations of the statutes they were disclosing to Judge Walker, was it also making expansive Executive Authority claims it couldn't (and still can't) share with plaintiffs? Did the government, for example, make an Executive Authority claim that we have every reason to believe John Bates (especially) and Reggie Walton would rebut if they knew about it?

In any case, in addition to the watchlist data from those 3,000 US persons (which would have aged off last month otherwise), the last of the illegal Internet content-as-metadata data might be aged off as soon as April absent these stays.That data might well provide plaintiffs proof they were illegally wiretapped (note, the Internet dragnet was limited to certain switches, but Jewel was built around the Folsom Street switch which was almost certainly included in that). And that the government provided highly misleading descriptions to

Vaughn Walker when bidding for a state secrets exemption.

And add in one more legal fight here: as I noted, DOJ is withholding the October 30, 2009 (as well as one later one from 2009) from both the ACLU and EFF (the EFF suit is before a different San Francisco judge). In addition, DOJ is refusing all push for expedited processing on FOIAs for the Internet dragnet filings.

Seeing how clearly manipulative their data release in these lawsuits is, it seems safe to suggest the government is also making FOIA decisions to prevent plaintiffs from obtaining information to really contest these suits. That shouldn't surprise anyone. But I would hope it would piss off the judges.

HOW THE NSA DEALS WITH A THREAT TO ITS BACKBONE HEGEMONY

I have talked before about the importance of US' dominant role in global telecom infrastructure in our hegemonic position.

> US hegemony rests on a lot of things: the dollar exchange, our superlative military, our ideological lip service to democracy and human rights.
>
> But for the moment, it also rests on the globalized communication system in which we have a huge competitive advantage. That is, one reason we are the world's hegemon is because the rest of the world communicates through us — literally, in terms of telecommunications infrastructure, linguistically, in English, and in terms of telecommunications governance.

Which is why these stories (NYT, Spiegel's short version, to be followed by a longer one Monday) about NSA's targeting of Huawei are so interesting. Der Spiegel lays out the threat Huawei poses to US hegemony.

> "We currently have good access and so much data that we don't know what to do with it," states one internal document. As justification for targeting the company, an NSA document claims that "many of our targets communicate over Huawei produced products, we want to make sure that we know how to exploit these products." The agency also states concern that "Huawei's widespread infrastructure will provide the PRC (People's Republic of China) with SIGINT capabilities." SIGINT is agency jargon for signals intelligence. The documents do not state whether the agency found information indicating that to be the case.
>
> The operation was **conducted with the involvement of the White House intelligence coordinator** and the FBI. One document states that the threat posed by Huawei is "unique".
>
> The agency also stated in a document that "the intelligence community structures are not suited for handling issues that combine economic, counterintelligence, military influence and telecommunications infrastructure from one entity."
>
> **Fears of Chinese Influence on the Net**
>
> **The agency notes that understanding how the firm operates will pay dividends in the future.** In the past, the network infrastructure business has been dominated by Western firms, but the Chinese are working to make American and Western firms "less relevant". That Chinese push is beginning to open up

> technology standards that were long determined by US companies, and China is controlling an increasing amount of the flow of information on the net. [my emphasis]

And the NSA document the NYT included makes this threat clear.

> There is also concern that Huawei's widespread infrastructure will provide the PRC with SIGINT capabilities and enable them to perform denial of service type attacks.

Now, for what it's worth, the NYT story feels like a limited hangout — an attempt to pre-empt what Spiegel will say on Monday, and also include a bunch of details on NSA spying on legitimate Chinese targets so the chattering class can talk about how Snowden is a tool of Chinese and Russian spies. (Note, the NYT story relies on interviews with a "half dozen" current and former officials for much of the information on legitimate Chinese targets here, a point noted by approximately none of the people complaining.)

But the articles make it clear that 3 years after they started this targeted program, SHOTGIANT, and at least a year after they gained access to the emails of Huawei's CEO and Chair, NSA still had no evidence that Huawei is just a tool of the People's Liberation Army, as the US government had been claiming before and since. Perhaps they've found evidence in the interim, but they hadn't as recently as 2010.

Nevertheless the NSA still managed to steal Huawei's source code. Not just so it could more easily spy on people who exclusively use Huawei's networks. But also, it seems clear, in an attempt to prevent Huawei from winning even more business away from Cisco.

I suspect we'll learn far more on Monday. But for now, we know that even the White House got

involved in an operation targeting a company that threatens our hegemony on telecom backbones.

FORMER NSA GENERAL COUNSEL ROBERT DEITZ, WHO RUBBER-STAMPED ILLEGAL WIRETAP PROGRAM, SAYS ALL FELONIES SHOULD BE PROSECUTED

I'm watching a CUNY conference on sources and secrets, which currently has a panel including Bob Woodward, Jane Mayer, and former NSA General Counsel Robert Deitz.

When asked whether he could think of a leak that had been damaging, Deitz said the exposure of the illegal (he called it "special") wiretap program had been damaging.

Then, in the context of prosecuting leaks, Deitz argued that all leaks should be prosecuted, because they involve a felony violation of an oath (that's not always true, but I'll just accept that Deitz believes all felonies should be prosecuted). He went on to say, "How is it you put a line around this felony and not prosecute it?"

According to the 2009 Draft NSA IG Report, Deitz, on September 20, 2001, suggested to Alberto Gonzales they should consider modifying FISA (which was then being modified as part of the PATRIOT Act); he appears to have gotten no

answer. On October 5, 2001 — having asked but not been permitted to read the underlying OLC authorization for it (Addington read him a few lines over the phone), having not participated in the drafting of the Presidential Authorization for it, and having given it just one day of legal review — Deitz said a program violating the exclusivity provision of FISA was legal. On October 8, Deitz briefed the analysts who would carry out this illegal program.

Deitz' subordinates provided the only oversight of the program at first. (Later in today's program he claimed the line between domestic and foreign intelligence was rigorously maintained.) To his credit, Deitz ultimately fought to have the Inspector General read into the program after it had operated for some months.

This is a man who provided the legal fig leaf for a patently illegal program (though the IG Report provides no details of Deitz' actions for the March to May 2004 timeframe, when the program was even more illegal). This is a man who showed awareness of the legally correct way to do this — include this expanded program in PATRIOT — but nevertheless accepted and participated in not doing so.

And he advocates prosecuting every felony.

Perhaps before he talks about prosecuting journalists and their sources, he should consider his own role in encouraging felonies?

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.

JOHN BRENNAN'S PARALLEL "INVESTIGATIVE, PROTECTIVE, OR INTELLIGENCE ACTIVITY"

Yesterday, Jack Goldsmith defended CIA lawyer Robert Eatinger for referring Senate Intelligence Committee staffers for criminal investigation. Eatinger had no choice but to refer his Agency's overseers, you see, because

EO 12333 required it.

> I knew Eatinger a bit when I was at OLC a decade ago, and based on that experience I agree with John Rizzo that "[h]e doesn't have a political bone in his body" and "[i]f he made this referral, it's because he felt it was the right and necessary thing to do."
>
> It might be useful to articulate the standard for the "right and necessary thing to do," because I think that standard is at the bottom of this corner of the controversy. The standard comes from Section 6.1(b) of E.O. 12,333, which imposes a duty on the CIA Director to:
>
> > Report to the Attorney General *possible* violations of Federal criminal laws by *employees and of specified Federal criminal laws by any other person* as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;
>
> I believe that the CIA Director delegates this duty to the CIA General Counsel.
>
> Note how low the bar is for the referral—*possible* violations of federal law. Think about what that low standard means. It means that CIA often has a duty to refer a matter to DOJ that it is reasonably confident does not violate federal law, simply because the matter possibly violates federal law. As John Radsan noted in his study of the CIA

> General Counsel's Office, the low standard results in CIA making "several referrals to the Justice Department in a typical month." It might seem that these frequent referrals are signs of lawlessness, but in fact they are a mechanism of accountability. The very soft trigger of "possible" as opposed to "likely" or "actual" violations promotes significant over-reporting and **allows another Agency, DOJ, to decide the appropriate action in the first instance**." [my emphasis]

Nice try.

But there's a significant problem with that. In response to Ron Wyden's question about whether CIA is subject to the Computer Fraud and Abuse Act — a polite way of suggesting CIA hacked the Committee server — John Brennan told Wyden,

> The statute does apply. The Act, however, expressly "does not prohibit any lawfully authorized investigative, protective, or intelligence activity … of an intelligence agency of the United States." 18 U.S.C. § 1030(f).

In other words, Brennan implicitly asserts the CIA snooping on SSCI was legal because CIA was engaged in lawfully authorized "investigative, protective, or intelligence activity."

Side note: what are the chances that Brennan, who likes to remind that he's not a lawyer when he gets legally dangerous questions, consulted with CIA's Acting General Counsel Robert Eatinger in crafting this response to Wyden?

But let's look at when and how Brennan chose to engage in what he claims is either "investigative, protective, **or** intelligence activity" and when and how Eatinger found SSCI's oversight of CIA reached the "low bar" that merited referral.

According to Dianne Feinstein, in 2010, before Brennan was Director and Eatinger Acting General Counsel, a slew of documents disappeared from the server CIA made available for SSCI. Feinstein makes no mention of CIA engaging in "investigative, protective, or intelligence activity" in response. Instead, CIA just made shit up.

> In May of 2010, the committee staff noticed that [certain] documents that had been provided for the committee's review were no longer accessible. Staff approached the CIA personnel at the offsite location, who initially denied that documents had been removed. CIA personnel then blamed information technology personnel, who were almost all contractors, for removing the documents themselves without direction or authority. And then the CIA stated that the removal of the documents was ordered by the White House. When the committee approached the White House, the White House denied giving the CIA any such order.
>
> After a series of meetings, I learned that on two occasions, CIA personnel electronically removed committee access to CIA documents after providing them to the committee. This included roughly 870 documents or pages of documents that were removed in February 2010, and secondly roughly another 50 were removed in mid-May 2010.

Only after denying it, then blaming first the IT contractors, and then the White House (who I believe may well have been to blame), did the CIA admit they had removed the documents. All this occurred, presumably, without launching a security review of the kind so urgent now (though if a security review were done, let's hear about it, because it would suggest only certain factions were behind the removal of these documents).

Shortly after this incident — again, according to Feinstein — the Panetta Review documents also started disappearing from the servers (SSCI either had printed out copies already or did so in response).

In December, Mark Udall and others started invoking the Panetta review and asking for a complete copy of it.

In response, according to a letter (which for a variety of reasons I'm certain was designed to be released) Brennan later sent Dianne Feinstein on January 27, CIA started its "investigative, protective, or intelligence activity."

> Because we were concerned that there may be a breach or vulnerability in the system for housing highly classified documents, CIA conducted a limited review to determine whether these files were located on the SSCI side of the CIA network and reviewed audit data to determine whether anyone had accessed the files, which would have been unauthorized. The technical personnel conducting the audit review were asked to undertake it only if it could be done without searching audit data relating to other files on the SSCI side of CIA's network. That review by IT personnel determined that the documents that you and Senator Udall were requesting appeared to already be on the SSCI staff side of CIA's local area network and had been accessed by staff. Only completion of the security review will answer how SSCI staff came into possession of the documents.

Only on January 15, after CIA had completed some of that "investigative, protective, or intelligence activity" and determined, according to them, that SSCI shouldn't have had the document, did Brennan call an "emergency meeting" to inform Feinstein and Saxby Chambliss of those activities.

> I made clear during our meeting that I wanted to conduct this security review with our consent and, furthermore, that I welcomed the participation of the Committee's Security Director in this effort.
>
> [snip]
>
> As I noted at our meeting, this is a very serious matter, and it is important that both the CIA and the Committee get to the bottom of what happened.

In response, according to Feinstein, she sent Brennan two letters, one, on January 17, objecting to CIA's "investigative, protective, or intelligence activity," and the second, on January 23, asking specific questions about what CIA had done.

> Two days after the meeting, on January 17, I wrote a letter to Director Brennan objecting to any further CIA investigation due to the separation of powers constitutional issues that the search raised. I followed this with a second letter on January 23 to the director, asking 12 specific questions about the CIA's actions—questions that the CIA has refused to answer.
>
> Some of the questions in my letter related to the full scope of the CIA's search of our computer network. Other questions related to who had authorized and conducted the search, and what legal basis the CIA claimed gave it authority to conduct the search. Again, the CIA has not provided answers to any of my questions.
>
> My letter also laid out my concern about the legal and constitutional implications of the CIA's actions. Based on what Director Brennan has informed us, I have grave concerns that the CIA's search may well have violated the

> separation of powers principles embodied in the United States Constitution, including the Speech and Debate clause. It may have undermined the constitutional framework essential to effective congressional oversight of intelligence activities or any other government function.

The letter Brennan has released (which, as I have said, seems designed for release) did not answer these questions or even acknowledge they had been asked. Instead, Brennan insisted that CIA's "investigative, protective, or intelligence activity" continue, though invited another, independent inquiry with Committee involvement.

> I would welcome an independent review that explores CIA's actions and how these documents came to reside on the Committee's side of the CIA facility network. If you are amenable, I will have my Acting General Counsel reach out to the Committee's Majority and Minority Counsel to discuss options for such an independent review.
>
> However we proceed, the security review must be completed in a timely manner. It is imperative to learn whether or not a breach or vulnerability exists on this network and was exploited. I trust that you share my concerns and that we can work together to carry out a security review that answers these important questions while respecting the important separation of powers concerns of both.

According to both accounts, there had been no mention of involving DOJ up to that point.

Meanwhile, CIA's Inspector General David Buckley started an investigation and ultimately referred it to DOJ, and then in response, Robert Eatinger referred the SSCI to DOJ.

> Days after the meeting with Director Brennan, the CIA inspector general, David Buckley, learned of the CIA search and began an investigation into CIA's activities. I have been informed that Mr. Buckley has referred the matter to the Department of Justice given the possibility of a criminal violation by CIA personnel.
>
> Let me note: because the CIA has refused to answer the questions in my January 23 letter, and the CIA inspector general review is ongoing, I have limited information about exactly what the CIA did in conducting its search.
>
> Weeks later, I was also told that after the inspector general referred the CIA's activities to the Department of Justice, the acting general counsel of the CIA filed a crimes report with the Department of Justice concerning the committee staff's actions. I have not been provided the specifics of these allegations or been told whether the department has initiated a criminal investigation based on the allegations of the CIA's acting general counsel.

In other words, Eatinger didn't refer this case when CIA first started worrying about possible violations of Federal law (nor, as far as we know, did Stephen Preston make a referral in 2010 when documents started disappearing from the server). He didn't refer the case after CIA's initial "investigative, protective, or intelligence activity" — at that point, Brennan still wanted CIA to continue its "investigative, protective, or intelligence activity" itself.

It was only after CIA got referred for its "investigative, protective, or intelligence activity" that Eatinger decided the matter had reached what Goldsmith claims is a very low bar for referral.

Now, I might entertain the possibility that after things started spinning out of control, Eatinger got the brilliant idea that it was not a good idea for CIA to conduct "investigative, protective, or intelligence activity" targeted at their overseers. It's possible, too, that Brennan envisioned the "independent investigation" mentioned in his letter to Feinstein would be conducted by DOJ, though he didn't say that in his letter that I believe was designed to be publicly released.

But certainly, Eatinger let things get far beyond the "low bar" before he referred the issue to DOJ. He certainly didn't let another Agency "decide the appropriate action in the first instance." CIA got to decide that.

Which brings me to the even more troubling aspect of this.

Given Brennan's response to Wyden (which may or may not have been written after consultation with Eatinger), the CIA Director believes the limits on EO 12333 do not prevent the CIA from conducting its own parallel "investigative, protective, or intelligence activity" outside the realm of normal law enforcement, **not even** if CIA was directly involved.

Say, did you notice that Brennan didn't specify for Wyden whether he believed CIA had been engaged in "investigative" or "protective" or "intelligence" activity?

CIA's not supposed to be in charge of intelligence activities targeted at Americans — FBI is, the same investigative agency only now being involved in this, in spite of the "low bar" on referrals under EO 12333.

Suffice it to say it might have behooved Brennan, given that he edited the citation from 18 U.S.C. § 1030(f), to specify what kind of authorized activity CIA was engaged in when it snooped on its overseers.

Because the impression I get from all this is that the Director of the CIA thinks it's

perfectly okay for CIA to conduct its own "investigative, protective, or intelligence activity" in parallel with more appropriate means of investigating events involving CIA. (Think, for example, of the potentially parallel investigation it might conduct of Gitmo detainees and their lawyers as they discuss torture using bugs in the smoke alarms and a kill switch on the white noise machine?) And this was targeted at its overseers! Imagine the extent of "investigative, protective, or intelligence activity" CIA might engage in if it was someone without the purported protections of Separation of Powers.

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.