THE HOSPITAL CONFRONTATION HEROES OF RULE OF LAW GUTTED SEPARATION OF POWERS

Remember that cinematic story of how Jim Comey and Jack Goldsmith and Robert Mueller stood up to Bush and Cheney and forced them to shut down their illegal dragnet to defend the rule of law in 2004?

It turns out, what Comey and Goldsmith did in secret two months later was not so heroic. As I lay out over at Salon, the memo of law they used to get their illegal dragnet blessed by the FISA court argued both Judge Colleen Kollar-Kotelly and the Congress that passed the PRTT law in the first place had no choice but to cede to Executive power.

> Essentially, they argued both she — an Article III judge — and Congress must have their power gutted to protect the president's power.
>
> [snip]
>
> The same heroes of the hospital confrontation, lionized for the last decade for their courageous defense of the rule of law, thereby gutted the separation of powers, in secret. All to serve still more secrecy … and the power of the presidency they purportedly reined in two months earlier.
>
> They may have won Bush — and themselves, who otherwise would have signed off on an illegal program — legal cover by doing so. But in the process they corroded the balance of powers

> enshrined by the Constitution, turning the FISC into a place where expansive executive branch programs get rubber-stamped in secret.

Here's how they justified not getting Congress to write a new law to authorize the spying they themselves refused to approve.

> The memo's focus on Congress — at least what appears in unredacted form — is much more circumspect, but perhaps even more disturbing.
>
> DOJ pointed to language showing Congress intended pen registers to apply to the Internet; they pointed to the absence of language prohibiting a pen register from being used to collect data from more than a single user, as if that's the same as collecting from masses of people and as if that proved congressional intent to wiretap everyone.
>
> And then they dismissed any potential constitutional conflict involved in such broad rereadings of statutes passed by Congress. "In almost all cases of potential constitutional conflict, if a statute is construed to restrict the executive, the executive has the option of seeking additional clarifying legislation from Congress," the heroes of the hospital confrontation admitted. The White House had, in fact, consulted Majority Leader Tom DeLay about doing just that, but he warned it would be too difficult to get new legislation. So two months later, DOJ argued Congress' prerogative as an independent branch of government would just have to give way to secrecy. "In this case, by contrast, the Government cannot pursue that route because seeking legislation would inevitably compromise the secrecy of the collection program the Government wishes

> to undertake.”

You remember that part of the Constitution where it says Congress passes the laws, unless the Executive Branch wants the laws to be secret, in which case they can do it?

Nope, neither do I.

INTERNET DRAGNET MATERIALS, WORKING THREAD 1

I Con the Record just released some ridiculously overclassified Internet dragnet documents it claims shows oversight but which actually shows how they evaded oversight. I’ve added letters to ID each document (I’ll do a post rearranging them into a timeline tomorrow or soon thereafter).

For a timeline I did earlier of the Internet dragnet program see this post.

This will be the first of several working threads, starting with descriptions of what we’ve got.

8/12: Note I will be updating this as I can clarify dates and content.

So-called Judicial oversight

A. FISC Opinion and Order: This is the Kollar-Kotelly order that initially approved the dragnet on July 14, 2004. A searchable version is here.

B. FISC Primary Order: This is an Internet

dragnet order signed by Reggie Walton, probably in 2008 or very early 2009. It shows that the Internet dragnet program, which was almost certainly illegal in any case, had less oversight than the phone dragnet program (though at this point also collected fewer records). It was turned over pursuant to FAA requirements on March 13, 2009.

C. FISC Primary Order: This is an Internet dragnet order probably from May 29, 2009 (as identified in document D), signed by Reggie Walton. It shows the beginning of his efforts to work through the Internet violations. It appears to have been provided to Congress on August 31, 2009.

D. FISC Order and Supplemental Order: This is a version of the joint June 22, 2009 order released on several occasions before. It shows Reggie Walton's efforts to work through the Internet dragnet violations. Here's one version.

E. FISC Supplemental Order: This appears to be the dragnet order shutting down dragnet production. It would date to fall 2009 (production was likely shut down in October 2009, though this might reflect the initial shut-down).

F. FISC Primary Order: I'm fairly sure this is an order from after Bates turned the Internet dragnet back on in 2010 (and is signed by him), though I will need to verify that. It does require reports on how the NSA will segregate previously violative records, which is consistent with it dating to 2011 sometime (as is the requirement that the data be XML tagged).

G. FISC Memorandum Opinion Granting in Part and Denying in Part Application to Reinitiate, in Expanded Form, Pen Register/Trap and Trace Authorization: This is the order, from sometime between July and October 2010, where John Bates turned back on and expanded the Internet dragnet. Here's the earlier released version (though I think it is identical).

H. Declaration of NSA Chief, Special FISA

Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency: This was a report Walton required in document C, above, and so would be in the May-June 2009 timeframe. Update: Likely date June 18, 2009.

I. Government's Response to the FISC's Supplemental Order: This is the government's response to an order from Walton, probably in his May 29, 2009 opinion (see this order for background), or even earlier in May.Update: This response dates to June 18, 2009 or slightly before.

J. Declaration of NSA Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency: This appears to be the declaration submitted in support of Response I and cited in several places. Update: likely date June 18, 2009.

K. Supplemental Declaration of Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency: This appears to be the declaration that led to document C above.

L. Government's Response to the FISC's Supplemental Order Requesting a Corrective Declaration: This is a declaration admitting dissemination outside the rules responding to 5/29 order.

M. Government's Response to a FISC Order: This is the government's notice that it was using automatic queries on Internet metadata, just as it also was with the phone dragnet. This notice was provided to Congress in March 2009.

N. Declaration of Lieutenant General Keith B. Alexander, U.S. Army, Director, NSA, Concerning NSA's Compliance with a FISC Order: After Walton demanded declarations in response to the initial phone dragnet violation, he ordered NSA to tell him whether the Internet dragnet also had the same problems. This is Keith Alexander's declaration describing the auto scan for that

program too. It was provided to Congress in March 2009.

O. Preliminary Notice of Potential Compliance Incident: This is the first notice of the categorical violations that ultimately led to the temporary shutdown of the dragnet, in advance of order E.

P. Notice of Filing: This is notice of a filing in response to inquiry from Judge Walton. It could be from any time during David Kris' 2009 to early 2011 tenure.

Q: Government's Application for Use of Pen Register/Trap and Trace Devices for Foreign Intelligence Purposes: ~~This appears to be the application following Order E, above. I don't think it's the 2010 application that led to the reauthorization of the dragnet, because it refers to facilities whereas the 2010 order authorized even broader collection. (Remember Bates' 2010 order said the government applied, but then withdrew, an application.)~~ Update and correction: this application must post-date December 2009, because that's when NSA changed retention dates from 4.5 years to 5. Also note reference to change in program and request to access illegally collected data from before 10/09.

R. Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes: This appears to be the memorandum of law accompanying application Q.

S. Declaration of General Keith B. Alexander, U.S. Army, Director, NSA, in Support of Pen Register/Trap and Trace Application: This is Alexander's declaration accompanying Q.

T. Exhibit D in Support of Pen Register/Trap and Trace Application: This is a cover letter. I'm not sure whether it references prior communications or new ones.

U. First Letter in Response to FISC Questions Concerning NSA bulk Metadata Collection Using

Pen Register/Trap and Trace Devices: This is the first of several letters in support of reinitiation of the program. The tone has changed dramatically here. For that reason, and because so much of it is redacted, I think this was part of the lead-up to the 2010 reauthorization.

V. Second Letter in Response to FISC Questions concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices: This second letter is entirely redacted except for the sucking up to Bates stuff.

W. Third Letter in Response to FISC Questions Concerning NSA Bulk Metadata Collection Using Pen Register/Trap and Trace Devices: More sucking up. Some language about trying to keep access to the existing illegally collected data.

X. Application for Pen Register/Trap and Trace Devices for Foreign Intelligence Purposes: This is the first application for the Internet dragnet, from 2004. Very interesting. Note it wasn't turned over until July 2009, after Congress was already learning of the new problems with it.

Y. Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes: The memorandum of law accompanying X. Also turned over to Congress in 2009.

Z. Declaration of General Michael V. Hayden, U.S Air Force, Director, NSA, in Support of Pen Register/Trap and Trace Application: This goes with the initial application. NSA has left stuff unredacted that suggests they were access less bandwith than they, in the end, were. Also remember NSA violated this from the very beginning.

AA. Application for Use of Pen Register/Trap and Trace Devices for Foreign Intelligence Purposes: ~~This appears to be the application for the second PRTT order. I'll return to this~~

~~tomorrow, but I don't think it reflects the violation notice it should.~~

BB. Declaration of NSA Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate: ~~This is NSA's declaration in conjunction with the first reapplication for the dragnet. This should have declared violations. It was turned over to Congress in March 2009.~~ [update: these appear to be early 2009 application]

CC. Declaration Lieutenant General Keith B. Alexander, U.S. Army, Director, NSA, Concerning NSA's Implementation of Authority to Collect Certain Metadata: This is Alexander's declaration accompanying the End-to-End report, from sometime in fall 2009.

DD: NSA's Pen Register Trap and Trace FISA Review Report: The end-to-end report itself. it was provided to Congress in January 2010.

EE: DOJ Report to the FISC NSA's Program to Collect Metadata: DOJ's accompaniment to the end-to-end report.

FF: Government's First Letter to Judge Bates to Confirm Understanding of Issues Relating to the FISC's Authorization to Collect Metadata: After Bates raauthorized the Internet dragnet, DOJ realized they might not be on the same page as him. Not sure if this was in the 2009 attempt or the 2010 reauthorization.

GG: Government's Second Letter to Judge Bates to Confirm Understanding of Issues Relating to the FISC's Authorization to Collect Metadata: A follow-up to FF.

HH: Tab 1 Declaration of NSA Chief, Special Oversight and Processing, Oversight and Compliance, Signals Intelligence: This appears to be the 90-day report referenced in document C. Update: Actually it is referenced in Document A: note the paragraphs describing the chaining that were discontinued before the dragnet approval.

II: Verified Memorandum of Law in Response to FISC Supplemental Order: This is one of the most fascinating documents of all. It's a 2009-2011 (I think August 17, 2009, though the date stamp is unclear) document pertaining to 3 PRTT targets, relying on criminal PRTT law and a 2006 memo that might be NSA's RAS memo (though the order itself is FBI, which makes me wonder whether it seeds the FBI program). It may have been what they used to claim that Internet content counted as metadata.

JJ: Memorandum of Law in Response to FISC Order: A September 25, 2006 response to questions from the FISC, apparently regarding whether rules from criminal pen registers apply to PATRIOT PRTT. While I think this addresses the application to Internet, I also think this language may be being used for location.

So-called Congressional oversight

KK: Government's Motion to Unseal FISC Documents in Order to Brief Congressional Intelligence and Judiciary Committees: This is a request to unseal an order — I suspect document E — so it could be briefed to Congress.

LL: Order Granting the Government's Motion to Unseal FISC Documents in Order to Brief Congressional Intelligence and Judiciary Committees: Walton's order to unseal KK for briefing purposes.

MM: April 27, 2005 Testimony of the Attorney General and Director, FBI Before the Senate Select Committee on Intelligence: This is the 2005 testimony in which — I pointed out before — Alberto Gonzales did not brief Congress about the Internet dragnet.

So-called Internal oversight

NN: NSA IG Memo Announcing its Audit of NSA's Controls to Comply with the FISA Court's Order Regarding Pen Register/Trap and Trace Devices: This lays out an audit with PRTT compliance, noting that the audit also pertains to BR FISA (phone dragnet). It admits the audit was shut down when the order was not renewed. It's unclear whether this was the 2009 or the 2011 shutdown, but the implication is it got shut down because it would not pass audit.

OO: NSA IG Memo Suspending its Audit of NSA after the NSA's PRTT Metadata Program Expired: the formal announcement they were shutting down the IG report. Again, it's not clear whether this was the 2009 or the 2011 shutdown.

If you find this work valuable, please consider donating to support the work.

USA FREEDOM DOES NOT REIN IN THE SPIES

Honest. I started writing about this David Cole column asking, "Can Congress rein in the spies?" before John Brennan admitted that, contrary to his earlier assurances, his spooks actually had been spying on their Congressional overseers and also before President Obama announced that, nevertheless, he still has confidence in Brennan.

Cole's column isn't about the the Senate Intelligence Committee's struggles to be able to document CIA torture, however. It's about how Patrick Leahy introduced his version of USA Freedom Act "not a moment too soon."

I don't want to gripe with the column's presentation of Leahy's version of Freedom; with a few notable exceptions (one which I'll get to), it accurately describes how Leahy's bill improves on the bill the spies gutted in the House.

I first wanted to point to why Cole says Leahy's bill comes not a moment too soon.

> Leahy's bill comes not a moment too soon. Two reports issued on Monday bring into full view the costs of a system that allows its government to conduct dragnet surveillance without specific suspicions of wrongdoing. In *With Liberty to Monitor All*, Human Rights Watch and the ACLU make a powerful case that mass surveillance has already had a devastating effect on journalists' ability to monitor and report on national security measures, and on lawyers' ability to represent victims of government overreaching. And the same day, the New America Foundation issued *Surveillance Costs*, a report noting the widespread economic harm to US tech companies that NSA surveillance has inflicted, as potential customers around the world take their business elsewhere.
>
> Together, these reports make concrete the damaging effects of out-of-control surveillance, even to those with "nothing to hide." Our democracy has long rested on a vibrant and vigorous press and open legal system. On matters of national security, journalists probably serve as a more important check on the executive than even the courts or Congress.
>
> [snip]
>
> And, it turns out, tech companies also need to be able to promise confidentiality. Customers of Internet

> services or cloud computing storage programs, for example, expect and need to be certain that their messages and stored data will be private. Snowden's revelations that the NSA has been collecting vast amounts of computer data, and has exploited vulnerabilities in corporate encryption programs, have caused many to lose confidence in the security of American tech companies in particular.

Cole describes the great costs out-of-control surveillance imposes on journalists, lawyers, and cloud providers, and implies we cannot wait to reverse those costs.

Then he embraces a bill that would not protect journalists' conversations with whistleblowers (Leahy's Freedom still permits the traditional access of metadata for counterintelligence purposes as well as the Internet dragnet conducted overseas) or alleged terrorists, would not protect lawyers' discussions with their clients (the known attorney-client protected collections happened under traditional FISA, EO 12333, and possibly Section 702, none of which get changed in this bill), and would expose American companies' clouds even further to assisted government access under the new Call Detail Record provision.

Cole does admit the bill does not address Section 702; he doesn't mention EO 12333 at all, even though both the HRW and NAF reports did.

> Senator Leahy's bill is not a cure-all. It is primarily addressed to the collection of data within the United States, and does little to reform Section 702, the statute that authorizes the PRISM program and allows the government to collect the content of electronic communications of noncitizens abroad, even if they are communicating with US citizens here. And it says nothing about the NSA's deeply troubling

> practice of inserting vulnerabilities into encryption programs that can be exploited by any hacker. It won't, therefore, solve all the problems that the HRW and New American Foundation reports identify. But it would mark an important and consequential first step.

But he doesn't admit the bill does little to address the specific sources of the costs identified in the two reports. It's not a minute too soon to address these costs, he says, but then embraces a bill that doesn't really address the actual sources of the costs identified in the reports.

That is mostly besides the point of whether Leahy's bill is a fair apples-to-oranges trade-off with the status quo as to represent an improvement — an answer to which I can't yet give, given some of the obvious unanswered questions about the bill. It is, however, a testament to how some of its supporters are overselling this bill and with it anyone's ability to rein in the intelligence community.

But it's one testament to that that bugs me most about Cole's column. As I noted, he does mention Leahy's failure to do anything about Section 702. Nowhere in his discussion of 702, however, does he mention that it permits warrantless access to Americans' content, one which FBI uses when conducting mere assessments of Americans. Which of course means Cole doesn't mention the most inexcusable part of the bill — its exemption on already soft reporting requirements to provide the numbers for how many Americans get exposed to these back door searches.

I'm not a fancy Georgetown lawyer, but I strongly believe the back door searches — conducted as they are with no notice to anyone ultimately prosecuted based off such information — are illegal, and probably unconstitutional. When retired DC Circuit Court judge Patricia Wald raised these problems with the practice, Director of National Intelligence Counsel Bob

Litt simply said it would be "impracticable" to add greater oversight to back door searches. And in spite of the fact that both the President's Review Group and PCLOB advised significant controls on this practice (which implicates the costs identified in both the HRW and NAF reports), the version of USA Freedom Act crafted by the head of the Senate Judiciary Committee — the Committee that's supposed to ensure the government follows the law — not only doesn't rein in the practice, but it exempts the most egregious part of the practice from the transparency applauded by people like Cole, thereby tacitly endorsing the worst part of the practice.

And all that's before you consider that the IC also conducts back door searches of EO 12333 collected information — as first reported by me, but recently largely confirmed by John Napier Tye. And before you consider the IC's explicit threat — issued during the passage of the Protect America Act — that if they don't like any regulation Congress passes, they'll just move the program to EO 12333.

The point is, Congress *can't* rein in the IC, and that's only partly because (what I expect drives the Senate's unwillingness to deal with back door searches) many members of Congress choose not to. The have not asserted their authority over the IC, up to and including insisting that the protections for US persons under FISA Amendments Act actually get delivered.

In response to the news that Brennan's spies had been spying on its Senate overseers, Patrick Leahy (who of course got targeted during the original PATRIOT debate with a terrorist anthrax attack) issued a statement insisting on the importance of Congressional oversight.

> Congressional oversight of the executive branch, without fear of interference or intimidation, is fundamental to our Nation's founding principle of the separation of powers.

Yet his bill — which is definitely an improvement over USA Freedumber but not clearly, in my opinion, an improvement on the status quo — tacitly endorses the notion that FBI can conduct warrantless searches on US person communications without even having real basis for an investigation.

That's not reining in the spies. That's blessing them.

HAVING BEEN ABSOLVED BY DOJ, CIA NOW ADMITS THEY ILLEGALLY SPIED ON SSCI

When Ron Wyden first asked John Brennan whether CIA had to comply with the Computer Fraud and Abuse Act, Brennan suggested they didn't have to if they were conducting investigations.

> 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).

Then in March, after Senator Feinstein accused the CIA of improperly spying on her committee, Brennan claimed it was outside the realm of possibility.

> As far as the allegations of, you know, CIA hacking into, you know, Senate computers, nothing could be further from the truth. I mean, we wouldn't do that. I mean, that's — that's just beyond the — you know, the scope of reason in terms of what we would do.

Now that DOJ has decided not to investigate CIA's illegal domestic spying, we learn it was well within the realm of possibility.

> CIA employees improperly accessed computers used by the Senate Intelligence Committee to compile a report on the agency's now defunct detention and interrogation program, an internal CIA investigation has determined.
>
> Findings of the investigation by the CIA Inspector General's Office "include a judgment that some CIA employees acted in a manner inconsistent with the common understanding reached between SSCI (Senate Select Committee on Intelligence) and the CIA in 2009," CIA spokesman Dean Boyd said in a statement.

Brennan's solution is to have corrupt hack Evan Bayh conduct an accountability review of the spying.

Mark Udall and Ron Wyden are furious. DiFi is less so. The Republicans on the Committee have been silent; apparently they're okay with CIA breaching separation of powers.

And yet again, the CIA proves it refuses to subsist within democratic structures.

NSA GOT INTO BED WITH THE SAUDIS JUST BEFORE OUR TECHNICAL COOPERATION

AGREEMENT EXPANDED

In February 2011, around the time the CIA took over the hunt for Anwar al-Awlaki, NSA started collaborating with Saudi Arabia's Ministry of Interior's (MOI) Technical Assistance Directorate (TAD), under the umbrella of CIA's relationship with MOI (it had previously cooperated primarily with the Kingdom's Ministry of Defense).

On August 15, 2011, hackers erased the data on two-thirds of the computers at Saudi Aramco; American sources claim Iran was the culprit.

On September 30, 2011, CIA killed Anwar al-Awlaki, using drones operated from a base on Saudi soil.

On November 5, 2012, King Abdullah named close John Brennan ally Mohammed bin Nayef (MbN) Minister of the Interior; MbN had for some time been our top counterterrorism partner in the Kingdom.

On December 11, 2012, James Clapper expanded NSA's Third Party SIGINT relationship with the Kingdom of Saudi Arabia, for the first time formally including the Ministry of Interior's Technical Affairs Directorate.

Between January 14 and 16, 2013 MbN traveled to Washington and met with just about every top National Security person (many of whom, including Brennan, were just assuming new jobs). On January 16, MbN and Hillary Clinton renewed and expanded the Technical Cooperation Agreement initiated in 2008. The TCA was modeled on the JECOR program used from the late 1970s until 2000 to recycle US dollars into development programs in Saudi Arabia; in this more recent incarnation, the Saudis recycle dollars into things like a 30,000 mercenary army and other military toys for internal stability and border control. Last year's renewal — signed just over a month after Clapper made the Saudis full Third Person partners — added cybersecurity to the portfolio. The TCA — both the existing security

resources and its expansion under close ally MbN — shored up the power base of one of our closest partners (and at a time when we were already panicking about Saudi succession).

In other words, in addition to expanding Saudi capabilities at a time when it has been cracking down on peaceful dissent, which is what the Intercept story on this document discusses, by giving the Saudi MOI Third Party status, we added to the power of a key ally within the royal family, and did so at a time when the TCA was already shoring up his power base.

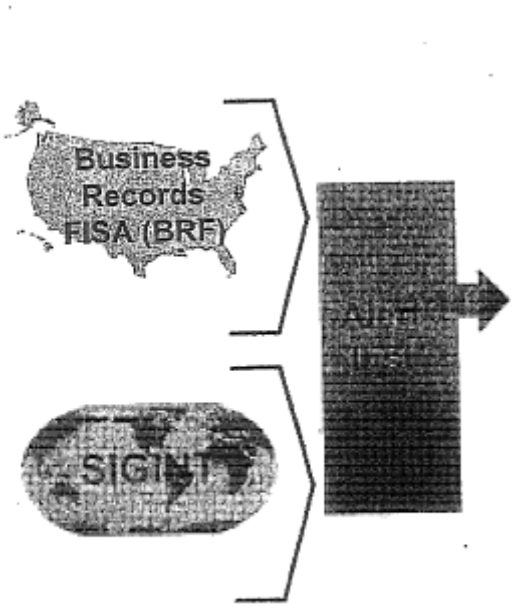
We did so, the Information Paper makes clear, in part because MOI has access to internal Saudi telecommunications. While the Information paper talks about AQAP and Iran's Republican Guard, they are also targeting Saudi targets.

And these new capabilities? They get coordinated through Chief of Station in Riyadh, the CIA. John Brennan's agency.

It's all very tidy, don't you think?

NSA'S DISINGENUOUS CLAIMS ABOUT EO 12333 AND THE FIRST AMENDMENT

Thanks to John Napier Tye's Sunday op-ed, some surveillance watchers are just now discovering EO 12333, which I've written some 50 posts about over the last year.



Back in January, I focused on one of the most alarming disclosures of the 2009 phone dragnet problems, that 3,000 presumed US person identifiers were on an alert list checked against each day's incoming phone dragnet data. That problem — indeed, many of the problems reported at the beginning of 2009 — arose because the NSA dumped their Section 215 phone dragnet data in with all the rest of their metadata, starting at least as early as January 4, 2008. It took at least the better part of 2009 for the government to start tagging data, so the NSA could keep data collected under different authorities straight, though once they did that, NSA trained analysts to use those tags to bypass the more stringent oversight of Section 215.

One thing that episode revealed is that US person data gets collected under EO 12333 (that's how those 3,000 identifiers got on the alert list), and there's redundancy between Section 215 and EO 12333. That makes sense, as the metadata tied to the US side of foreign calls would be collected on collection overseas, but it's a detail that has eluded some of the journalists making claims about the scope of phone dragnet.

Since I wrote that early January post, I've been meaning to return to a remarkable exchange from the early 2009 documents between FISC Judge Reggie Walton and the government. In his order for more briefing, Walton raised questions about tasking under NSA's SIGNIT (that is, EO 12333) authority.

> The preliminary notice from DOJ states that the alert list includes telephone identifiers that have been tasked for collection in accordance with NSA's SIGINT authority. What standard is applied for tasking telephone identifiers under NSA's SIGINT authority? Does NSA, pursuant to its SIGINT authority, task telephone identifiers associated with United States persons? If so, does NSA limit such identifiers to those that were not selected solely upon the basis of First Amendment protected activities?

The question reveals how little Walton — who had already made the key judgments on the Protect America Act program 2 years earlier — knew about EO 12333 authority.

I've put NSA's complete response below the rule (remember "Business Records" in this context is the Section 215 phone dragnet authority). But basically, the NSA responded,

- Even though the alert list included IDs that had not been assessed or did not meet Reasonable Articulable Suspicion of a tie to one of the approved terrorist groups, they at least had to have foreign intelligence value. And occasionally NSA's counterterrorism people purge the list of

non-CT IDs.

- Usually, NSA can only task (a form of targeting!) a US person under a FISA authority.
- Under EO 12333 and other related authorities, NSA can collect SIGINT information for foreign and counterintelligence purposes; its collection, retention, and dissemination of US person is governed by Department of Defense Regulation 5240.1-R and a classified annex. (see page 45 for the unclassified part of this)
- Since 2008, if the NSA wants to target a US person overseas they need to get and comply with a FISA order.
- NSA provides First Amendment protection in two ways – first, by training analysts to spy "with full consideration of the rights of United States persons."
- NSA provides First Amendment protection under EO 12333 by prohibiting NSA "from collecting or disseminating information concerning US persons' 'domestic activities' which are defined as 'activities that

> take place in the domestic United States that do not involve a significant connection to a foreign power, organization, or person.'"

The First Amendment claims in the last two bullets are pretty weak tea, as they don't actually address First Amendment issues and contact chaining is, after all, chaining on associations.

That's all the more true given what we know had already been approved by DOJ. In the last months of 2007, they approved the contact chaining through US person identifiers of already-collected data (including FISA data). They did so by modifying DOD 5240.1 and its classified annex so as to treat what they defined (very broadly) as metadata as something other than interception.

> The current DOD procedures and their Classified Annex may be read to restrict NSA's ability to conduct the desired communications metadata analysis, at least with respect to metadata associated with United States persons. In particular, this analysis may fall within the procedures' definition of, and thus restrictions on, the "interception" and "selection" of communications. Accordingly, the Supplemental Procedures that would govern NSA's analysis of communications metadata expressly state that the DOD Procedures and the Classified Annex do not apply to the analysis of communications metadata. Specifically, the Supplemental Procedures would clarify that "contact chaining and other metadata analysis do not 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." Once approved, the Supplemental Procedures will clarify that the communications metadata analysis the NSA wishes to conduct is not restricted by the DOD procedures and their Classified Annex.

Michael Mukasey approved that plan just as NSA was dumping all the Section 215 data in with EO 12333 data at the beginning of 2008 (though they did not really roll it out across the NSA until later in 2009).

Nowhere in the government's self-approval of this alternate contact chaining do they mention First Amendment considerations (or even the domestic activities language included in their filing to Walton). And in the rollout, they explicitly permitted starting chains with identifiers of any nationality (therefore presumably including US person) and approved the use of such contact chaining for purposes other than counterterrorism. More importantly, they expanded the analytical function beyond simple contact chaining, including location chaining.

All with no apparent discussion of the concerns a FISC judge expressed when data from EO 12333 had spoiled Section 215 data.

We will, I expect, finally start discussing how NSA has been using EO 12333 authorities — and how they've represented their overlap with FISA authorized collection. This discussion is an important place to start.

(TS//SI//NF) Answer 5: SIGINT Tasking Standard: Although the alert list included telephone identifiers of counterterrorism targets that had not been assessed against the RAS standard [requiring a tie to specific, named terrorist organizations] or had been affirmatively determined by NSA personnel not to meet the RAS

standard, such identifiers were not tasked in a vacuum. Whether or not an identifier is assessed against the RAS standard, NSA personnel may not task an identifier for any sort of collection or analytic activity pursuant to NSA's general SIGINT authorities under Executive Order 12333 unless, in their professional analytical judgment, the proposed collection or analytic activity involving the identifier is likely to produce information of foreign intelligence value. In addition, NSA's counterterrorism organization conducted reviews of the alert list two (2) times per year to ensure that the categories (zip codes) used to identify whether telephone identifiers on the alert list remained associated with [redacted] or one of the other target sets covered by the Business Records Order. Also, on occasion the SIGINT Directorate changed an identifier's status from RAS approved to non-RAS approved-on the basis of new information available to the Agency.

(U) US Person Tasking: NSA possesses some authority to task telephone identifiers associated with US persons for SIGINT collection. For example, with the US person's consent, NSA may collect foreign communications to, from, or about the US person. In most cases, however, NSA's authority to task a telephone number associated with a US person is regulated by the FISA. For the Court's convenience, a more detailed description of the Agency's SIGINT authorities follows, particularly with respect to the collection and dissemination of information to, from, or about US persons.

(TS//SI//NF) NSA's general SIGINT authorities are provided by Executive Order 12333, as amended (to include the predecessors to the current Executive Order); National Security Council Intelligence Directive No. 6; Department of Defense Directive 5100.20; and other policy direction. In particular, Section 1.7(c) of Executive Order 12333 specifically authorizes NSA to "Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for

foreign intelligence and counterintelligence purposes to support national and departmental missions." However, when executing its SIGINT mission, NSA is only authorized to collect, retain or disseminate information concerning United States persons in accordance with procedures approved by the Attorney General. The current Attorney General approved procedures that NSA follows are contained in Department of Defense Regulation 5240.1-R, and a classified annex to the regulation governing NSA's electronic surveillance activities.

(U) Moreover, some, but not all, of NSA's SIGINT activities are also regulated by the Foreign Intelligence Surveillance Act. For example, since the amendment of the FISA in the summer of 2008, if NSA wishes to direct SIGINT activities against a US person located outside the United States, any SIGINT collection activity against the US person generally would require issuance of an order by the FISC. For SIGINT activities executed pursuant to an order of the FISC, NSA is required to comply with the terms of the order and Court-approved minimization procedures that satisfy the requirements of 50 U.S.C. § 1801(h).

(U) First Amendment Considerations: For the following reasons, targeting a US person solely on the basis of protected First Amendment activities would be inconsistent with restrictions applicable to NSA's SIGINT activities. As part of their annual intelligence oversight training, NSA personnel are required to re-familiarize themselves with these restrictions, particularly the provisions that govern and restrict NSA's handling of information of or concerning US persons. Irrespective of whether specific SIGINT activities are undertaken under the general SIGINT authority provided to NSA by Executive Order 12333 or whether such activity is also regulated by the FISA, NSA, like other elements of the US Intelligence Community, must conduct its activities "with full consideration of the rights of United States persons." See Section

1.1(a) of Executive Order 12333, as amended. The Executive Order further provides that US intelligence elements must "protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law." Id. at Section 1.1(b).

(U) Consistent with the Executive Order's requirement that each intelligence agency develop Attorney General approved procedures that "protect constitutional and other legal rights" (EO 12333 at Section 2.4), DoD Regulation 5240.1-R prohibits DoD intelligence components, including NSA, from collecting or disseminating information concerning US persons' "domestic activities" which are defined as "activities that take place in the domestic United States that do not involve a significant connection to a foreign power, organization, or person." See, e.g., Section C2.2.3 of DoD Regulation 5240.1-R, In light of this language, targeting a US person solely on the basis of protected First Amendment activities would be inappropriate.

EO 12333 THREATENS OUR DEMOCRACY

Among the many posts I've written about Executive Order 12333 — the order that authorizes all non-domestic spying — includes this post, where I noted that proposed changes to NSA's phone dragnet won't affect programs authorized by EO 12333.

> Obama was speaking **only** about NSA's treatment of Section 215 metadata, not the data — which includes a great amount of US person data — collected under

> Executive Order 12333.
>
> [snip]
>
> Section 215 metadata has different and significantly higher protections than EO 12333 phone metadata because of specific minimization procedures imposed by the FISC (arguably, **the program doesn't even meet the minimization procedure** requirements mandated by the law). We've seen the implications of that, for example, when the NSA **responded** to being caught watch-listing 3,000 US persons without extending First Amendment protection not by stopping that tracking, but simply cutting off the watch-list's ability to draw on Section 215 data.
>
> Basically, the way NSA treats data collected under FISC-overseen programs (including both Section 215 and FISA Amendments Act) is to throw the data in with data collected under EO 12333, but add query screens tied to the more strict FISC-regulations governing production under it.
>
> [snip]
>
> NSA's spokeswoman will say over and over that "everyday" or "ordinary" Americans don't have to worry about their favorite software being sucked up by NSA. But to the extent that collection happens under EO 12333, they have relatively little protection.

That's precisely the point made in an important op-ed by the State Department's former Internet freedom chief, John Napier Tye, who had access to data from EO 12333 collection.

> Bulk data collection that occurs inside the United States contains built-in protections for U.S. persons, defined as U.S. citizens, permanent residents and

> companies. Such collection must be authorized by statute and is subject to oversight from Congress and the Foreign Intelligence Surveillance Court. The statutes set a high bar for collecting the content of communications by U.S. persons. For example, Section 215 permits the bulk collection only of U.S. telephone metadata – lists of incoming and outgoing phone numbers – but not audio of the calls.
>
> Executive Order 12333 contains no such protections for U.S. persons if the collection occurs outside U.S. borders.
>
> [snip]
>
> Unlike Section 215, the executive order authorizes collection of the content of communications, not just metadata, even for U.S. persons. Such persons cannot be individually targeted under 12333 without a court order. However, if the contents of a U.S. person's communications are "incidentally" collected (an NSA term of art) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected U.S. persons be suspected of wrongdoing and places no limits on the volume of communications by U.S. persons that may be collected and retained.

Tye reveals that a document the White House provided to Congress said it had no intention of limiting back door searches of EO 12333 collected data because it would require too many changes to existing programs.

> In that document, the White House stated that adoption of Recommendation 12 [which would requiring purging US person data] would require "significant

> changes" to current practice under Executive Order 12333 and indicated that it had no plans to make such changes.

And Tye implies that NSA is using EO 12333 to conduct the Internet dragnet.

> All of this calls into question some recent administration statements. Gen. Keith Alexander, a former NSA director, has said publicly that for years the NSA maintained a U.S. person e-mail metadata program similar to the Section 215 telephone metadata program. And he has maintained that the e-mail program was terminated in 2011 because "we thought we could better protect civil liberties and privacy by doing away with it."Note, however, that Alexander never said that the NSA stopped collecting such data — merely that the agency was no longer using the Patriot Act to do so. I suggest that Americans should dig deeper.

I have made repeatedly covered SPCMA, the EO 12333 authorized Internet dragnet, which the government rolled out just as it was shutting down its PATRIOT-authorized Internet dragnet.

Because you've been reading me, you already knew what most others are only discovering because of this op-ed.

The most important point Tye made — it's one I've made too, but it can't be said enough — is this:

> The [Executive] order as used today threatens our democracy.

There is almost no oversight over this — and when Mark Udall suggested DOJ should exercise more of a role, the AAG for National Security showed no interest. This is the executive choosing to spy on Americans outside of all

oversight.

That's a threat to our democracy.

SNOWDEN'S SPIEGEL FILES, WORKING THREAD

I've decided the best way to digest the collection of documents released by Spiegel this week is to do a working thread. You can find links to the individual files here, or a very big PDF of all files here.

NSA, BND, BfV sharing

Note they describe using XKeyscore for "behavior detection techniques." Even in physical space, it's not clear current science supports the validity of such behavior detection. But this involves using someone's online behavior to translate "behavior" into suspicion.

In the list of topics they share on, there's Der Spiegel has redacted the place in "Europeans traveling to [redacted] to fight." That's presumably Syria (though could be Somalia). It'd be interesting to see the lead time on this international sharing and the time it shows up in news articles.

Note the reference to using XKeyscore for (German) domestic warranted content.

> In October 2011, SSG partnered with SUSLAG and BND to conduct a demonstration of XKEYSCORE to the BfV using BfV domestic warranted collection. The BND XKEYSCORE system successfully processed DSL wiretap collection belonging to a German domestic CT target.

I've long wondered whether they can use XKS for US domestic content. This would seem to suggest they can. It sort of makes you wonder whether they'd give XKS to telecoms under USA Freedumber?

Comprehensive internal summary of history

Note the other documents describe the partnership primarily in terms of CT, but this document makes it clear it also includes transnational crime and counternarcotics, Afghan support, and one redacted topic.

Note cyber is something that is later described as something NSA is pushing (in January 2013) to get BND to partner on. This document describes IAD as leading discussions at this point (January 2013); but described a follow-up meeting with NTOC and FAD that same month.

Note Germany's role in translating Igbo, left unredacted. This, and a number of other redacted references, seems to suggest the Germans play a key role in our collection and analysis of intelligence from Nigeria. Note, that might support the notion that one of the redacted sharing purposes is energy-related.

Germany appears to play a key role in our GSM collection. Note they also play a key role in VoIP, which may be why they were so interested in accessing Skype. Germany has already changed its privacy law to help us, but NSA isn't satisfied. I'm reminded of US Ambassador to Germany Philip Murphy's bitching about Germans not understanding the need to share information in the Internet era.

Beginnings of ESC

In 2012, Boundless Informant was going to soon roll out a "if you like this you'll like this" query suggestion mode.

Boundless Informant data does **not** include FISA or ECI (telecom partner) collection. So Boundless Informant is missing a lot.

Muscular, where NSA steals from Google overseas

(as well as Terrestrial RF) do not send their data back to NSA-W. I wonder if there are legal reasons for that.

The explanation for showing metadata rather than content is not included. I wonder why?

Agenda: Konen to NSA

Remember that AFRICOM was based in Europe before it moved. While this was before that time, EUROCOM had much of the continent at that point. So we should assume a lot of the NSA cooperation focuses on that.

Keith Alexander had been in charge of INSCOM during the years before this relationship was set up.

ESC becomes ESOC

This lists additional missions including Nigerian Energy Security (which would explain the focus on Igbo). I'm guessing that one of the redacted topics elsewhere is energy.

This also added Morocco, Algeria, Tunisia, and Libya as targets. I wonder if this location retained that role up to and through the Arab Spring?

NSA apparently used ESOC to track the 2006 Israeli assault on Lebanon.

I wonder whether the Pan Sahel movement missed a lot of the development of AQIM in the region?

Report on XKeyscore training

"Before the training, I was just happy to use it and not go to jail." [Um, hello.]

PRISM Reporting

The redacted topics are, per William Arkin, S2A: South Asia, S2B: China and Korea, S2H: Russia

I'll come back to what these data show later.

Tech Surveillance in Europe Africa

The Analytics for Identity Intelligence talks

about metadata for geolocation, content for confirmation. Interesting relationship if you're not supposed to get content to ID, as with US metadata.

Surveillance of African countries by JSA

This explains why US is willing to partner with Germany on Africa: They're advanced enough the US can share technology with them without giving them freebies. So they can pick up the Africa slack while the US is distracted in Afghanistan and Iraq.

JSA restrictions

This describes how, because JSA is not permitted to target EU countries or economic spying, the Germans presented a list of 31 companies that could not be targeted.

Processing differences

This is a May 2006 discussion of the difference in processing between BND and NSA. The former does more human analysis to pick what's important; the latter does more automatic processing at the packet level. The whole point of this is that NSA will pressure/impress BND to alter their approach, at least at the Joint effort.

> Full use of current NSA DNI processing systems and analysis methodologies at JSA will be key to influencing the BND to alter their strategic DNI processing approach.

Note, however, that the NSA approach involves more minimization based privacy, whereas the Germans use some kind of filter for privacy (I wonder if it's like ThinThread?). And they're forcing German to that approach.

Nymrod for matching name transcriptions

Russian names are not a priority—Arabic and Chinese are. And it's based off commercial software.

Nymrod presentation

Note the discussion of co-representation at 2

SUSLAG classification guide

Cover name for CSC is FIFTYEXCLAIM

XKeyscore

Note that Muscular is one of the British collections that goes to Stage 2 XKS, which is intended for very high volumes. That's the collection that steals from Google and Yahoo.

SID visits Germany

Note the reference to "leveraging language resources in UT," written well before the Data Center was started.

SADNESS IN THE NSA-TELECOM BROMANCE

In his report on an interview with the new Director of NSA, Admiral Mike Rogers, David Sanger gets some operational details wrong, starting with his claim that the new phone dragnet would require an "individual warrant."

The new phone dragnet neither requires "warrants" (the standard for an order is reasonable suspicion, not probable cause), nor does it require its orders to be tied to "individuals," but instead requires "specific selection terms" that may target facilities or devices, which in the past have been very very broadly interpreted.

All that said, I am interested in Rogers' claims

Sanger repeats about NSA's changing relationship with telecoms.

> He also acknowledged that the quiet working relationships between the security agency and the nation's telecommunications and high technology firms had been sharply changed by the Snowden disclosures — and might never return to what they once were in an era when the relationships were enveloped in secrecy.

Oh darn!

Sadly, here's where Sanger's unfamiliarity with the details makes the story less useful. Publicly, at least, AT&T and Verizon have had significantly different responses to the exposure of the dragnet (though that may only be because Verizon's name has twice been made public in conjunction with NSA's dragnet, whereas AT&T's has not been), and it'd be nice if this passage probed some of those details.

> Telecommunications businesses like AT&T and Verizon, and social media companies, now insist that "you are going to have to compel us," Admiral Rogers said, to turn over data so that they can demonstrate to foreign customers that they do not voluntarily cooperate. And some are far more reluctant to help when asked to provide information about foreigners who are communicating on their networks abroad. It is a gray area in the law in which American courts have no jurisdiction; instead, the agency relied on the cooperation of American-based companies.
>
> Last week, Verizon lost a longstanding contract to run many of the telecommunications services for the German government. Germany declared that the revelations of "ties revealed between foreign intelligence agencies

> and firms" showed that it needed to rely on domestic providers.

After all, under Hemisphere, AT&T wasn't requiring legal process even for *domestic* call records. I think it possible they've demanded the government move Hemisphere under the new phone dragnet, though if they have, we haven't heard about it (it would only work if they defined domestic drug dealer suspects as associated with foreign powers who have some tie to terrorism). Otherwise, though, AT&T has not made a peep to suggest they'll alter their decades-long overenthusiastic cooperation with the government.

Whereas Verizon has been making more audible complaints about their plight, long before the Germans started ending their contracts. And Sprint — unmentioned by Sanger — even demanded to see legal support for turning over phone data, including, apparently, turning over foreign phone data under ECPA;s exception in 18 U.S.C. § 2511(2)(f)'s permitting telecoms to voluntarily provide foreign intelligence data.

Given that background — and the fact ODNI released the opinions revealing Sprint's effort, if not its name — I am curious whether the telecoms are really demanding process. If courts really had no jurisdiction then it is unclear how the government could obligate production

Though that may be what the Microsoft's challenge to a government request for email held in Ireland is about, and that may explain why AT&T and Verizon, along with Cisco and Apple — for the most part, companies that have been more reticent about the government obtaining records in the US — joined that suit. (In related news, EU Vice President Viviane Reding says the US request for the data may be a violation of international law.)

Well, if the Microsoft challenge and telecom participation in the request for data overseas is actually an effort to convince the Europeans

these corporations are demanding legal process, Admiral Rogers just blew their cover.

> Admiral Rogers said the majority of corporations that had long given the agency its technological edge and global reach were still working with it, though they had no interest in advertising the fact.

Dear Ireland and the rest of Europe: Microsoft – which has long been rather cooperative with NSA, up to and including finding a way to obtain Skype data – may be fighting this data request just for show. Love, Microsoft's BFF, Mike Rogers.

VERIZON IN THE CLOUD

As a number of people have noted, Germany canceled its contract with Verizon for network services provided to the government.

> The German government on Thursday said it would end a contract with Verizon Communications Inc. because of concerns about network security, one of the most concrete signs yet that disclosures about U.S. spying were hurting American technology companies overseas.
>
> Germany will phase out Verizon's existing business providing communications services to government agencies by 2015, the Interior Ministry said. The winner in the decision:Deutsche Telekom, Verizon rival and German phone giant, which will take on those services.
>
> [snip]
>
> The U.S. telecom giant has been trying to head off a Snowden backlash from

> overseas customers since at least last fall, when its U.S. staff created NSA talking points for its offshore sales team, two people familiar with the matter said. The talking points included assertions the U.S. government didn't have direct access to Verizon's offshore data centers, that Verizon obeys local laws in whatever country it operates and that NSA data requests go through American judicial review, the people said.

For it's part, Verizon offered non-denial denials to questions about whether the US demanded foreign data from Verizon.

> Detlef Eppig, head of Verizon's German unit Verizon Germany said on Thursday: "Verizon Germany is a German company and we comply with German law."
>
> Verizon did not receive any demands from Washington in 2013 for data stored in other countries, the company said.
>
> "The U.S. government cannot compel us to produce our customers' data stored in data centres outside the U.S., and if it attempts to do so, we would challenge that attempt in a court," it added.
>
> The firm declined to comment on whether there had been requests in previous years.

Remember, starting in 2009, the phone dragnets specifically state that Verizon should not turn over foreign data under the phone dragnet (presumably in part, other details suggest, because obtaining the data under Section 215 would impose closer controls on the data).

This is interesting on its face.

But I'm most interested in how this is going to affect Verizon's stance towards US dragnets going forward. Already, it has been probably the

most reluctant of the telecoms since Snowden's leaks started. I even suspect that may have been one reason to split with Vodaphone.

There's reason to believe USA Freedumber primarily serves to obtain all of Verizon's cell data, which is the most important cell provider. And in a recent hearing, Verizon pushed back hard against being asked to retain their data, even while Senators seemed inclined to require it.

The phone dragnet debate is, to a significant extent, a negotiation between Verizon and the government.

And it just got put into the same position as all the PRISM providers —the cloud providers — where it is losing international business because of US demands. Which means, for the first time (even since 2008, where Internet companies tried to deny the telecoms which had been stealing from them immunity), a telecom has increasing reason to push back against the inevitable momentum toward crappy legislation.