

PROTECT AMERICA ACT WAS DESIGNED TO COLLECT ON AMERICANS, BUT DOJ HID THAT FROM THE FISC

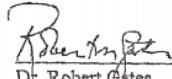
The government released a document in the Yahoo dump that makes it clear it intended to reverse target Americans under Protect America Act (and by extension, FISA Amendments Act). That's the Department of Defense Supplemental Procedures Governing Communications Metadata Analysis.

The document – as released earlier this month and (far more importantly) as submitted belatedly to the FISC in March 2008 – is fairly nondescript. It describes what DOD can do once it has collected metadata (irrespective of where it gets it) and how it defines metadata. It also clarifies that, “contact chaining and other metadata analysis do not qualify as the ‘interception’ or ‘selection’ of communications, nor to they qualify as ‘us[ing] a selection term’.”

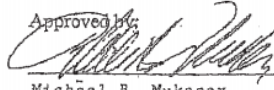
The procedures do not once mention US persons.

There are two things that should have raised suspicions at FISC about this document. First, DOJ did not submit the procedures to FISC in a February 20, 2008 collection of documents they submitted after being ordered to by Judge Walton after he caught them hiding other materials; they did not submit them until March 14, 2008.

The signature lines should have raised even bigger suspicions.


Dr. Robert Gates
Secretary of Defense

10-17-07
Date

Approved by:

Michael B. Mukasey
Attorney General
of the United States

1/3/08
Date

First, there's the delay between the two dates. Robert Gates, signing as Secretary of Defense, signed the document on October 17, 2007. That's after at least one of the PAA Certifications underlying the Directives submitted to Yahoo (the government is hiding the date of the second Certification for what I suspect are very interesting reasons), but 6 days after Judge Colleen Kollar-Kotelly submitted questions as part of her assessment of whether the Certifications were adequate. Michael Mukasey, signing as Attorney General, didn't sign the procedures until January 3, 2008, two weeks before Kollar-Kotelly issued her ruling on the certifications, but long after it started trying to force Yahoo to comply and even after the government submitted its first ex parte submission to Walton. That was also just weeks before the government redid the Certifications (newly involving FBI in the process) underlying PAA on January 29. I'll come back to the dates, but the important issue is they didn't even finalize these procedures until they were deep into two legal reviews of PAA and in the process of re-doing their Certifications.

Moreover, Mukasey dawdled two months before he signed them; he started at AG on November 9, 2007.

Then there's the fact that the title for his signature line was clearly altered, after the fact.

Someone else was supposed to sign these procedures. (Peter Keisler was Acting Attorney General before Mukasey was confirmed, including on October 17, when Gates signed these procedures.) These procedures were supposed to

be approved back in October 2007 (still two months after the first PAA Certifications) but they weren't, for some reason.

The backup to those procedures – which Edward Snowden leaked in full – may explain the delay.

Those procedures were changed in 2008 to reverse earlier decisions prohibiting contact chaining on US person metadata.

NSA had tried to get DOJ to approve that change in 2006. But James Baker (who was one of the people who almost quit over the hospital confrontation in 2004 and who is now FBI General Counsel) refused to let them.

After Baker (and Alberto Gonzales) departed DOJ, and after Congress passed the Protect America Act, the spooks tried again. On November 20, 2007, Ken Wainstein and Steven Bradbury tried to get the Acting Deputy Attorney General Craig Morford (not Mukasey, who was already AG!) to approve the procedures. The entire point of the change, Wainstein's memo makes clear, was to permit the contact chaining of US persons.

The Supplemental Procedures, attached at Tab A, would clarify that the National Security Agency (NSA) may analyze communications metadata associated with United States persons and persons believed to be in the United States.

What the government did, *after passage of the PAA*, was make it permissible for NSA to figure out whom Americans were emailing.

And this metadata was – we now know – central to FISC's understanding of the program (though perhaps not FISC's; in an interview today I asked Reggie Walton about this document and he simply didn't remember it).

The new declassification of the FISC opinion makes clear, the linking procedures (that is, contact chaining) NSA did were central to FISC's finding that Protect America Act, as implemented in directives to Yahoo, had

sufficient particularity to be reasonable.

The linking procedures – procedures that show that the [redacted] designated for surveillance are linked to persons reasonably believed to be overseas and otherwise appropriate targets – involve the application of “foreign intelligence factors” These factors are delineated in an ex parte appendix filed by the government. They also are described, albeit with greater generality, in the government’s brief. As attested by affidavits of the Director of the National Security Agency (NSA), the government identifies [redacted] surveillance for national security purposes on information indicating that, for instance, [big redaction] Although the FAA itself does not mandate a showing of particularity, see 50 U.S.C. § 1805(b). This pre-surveillance procedure strikes us as analogous to and in conformity with the particularly showing contemplated by Sealed Case.

In fact, these procedures were submitted to FISC and FISCER precisely to support their discussion of particularity! We know they were using these precise procedures with PAA because they were submitted to FISC and FISCER in defense of a claim that they weren’t targeting US persons.

Except, by all appearances, the government neglected to tell FISC and FISCER that the entire reason these procedures were changed, subsequent to the passage of the PAA, was so NSA could go identify the communications involving Americans.

And this program, and the legal authorization for it? It’s all built into the FISA Amendments Act.

RAEZ QADIR KHAN: HOISTING THE FBI ON ITS OWN METADATA PROBLEMS

Type	2005	2006	2007	2008	2009	2010	2011	2012	2013
Phone content									
Email content									
Cell phone content					September	January			
FedEx intercept					November				
Misc records									
Credit reports					September				
Wire transfers									
Call detail records									
Internet searches									
Bank records								September	
Residence									March

As I said earlier, the lawyers defending Pakistani-American Razez Qadir Khan – who is accused of material support of terrorist training leading up to an associate’s May 2009 attack on the ISI in Pakistan – are doing some very interesting things with the discovery they’ve gotten.

Request for Surveillance Authorities

The first thing they did, in a July 14, 2014 filing, was to list all the kinds of surveillance they’ve been shown in discovery with a list of possible authorities that might be used to conduct that surveillance. The motion is an effort to require the government to describe what it got how.

The table above is my summary of what the motion reveals and shows only if a particular kind of surveillance happened during a given year; it only gives more specific dates for one-time events.

The brown (orange going dark!) reflects that emails were turned over in discovery from this period, but that the 2013 search warrant apparently says “authorization to collect emails existed from August 2009 to May 2012.” That’s not necessarily damning; they could get those earlier emails legitimately via a number of

avenues that don't involve "collecting" them. But it is worth noting for reasons I explain below.

The filing itself includes tables with more specific dates, Bates numbers, possible authorities, and – where relevant – search warrant items reliant on the items in question. It also describes surveillance they know to have occurred – further Internet and email surveillance, for example, a 2009 search of Khan's apartment, as well as surveillance in later 2012 – that was not turned over in discovery.

Effectively, the motion lays out all the possible authorities that might be used to collect this data and then makes very visible that the criminal search warrant was derivative of it (there's a bit of a problem, because the warranted March 2013 search actually took place after the indictment, and so Khan's indictment can't be entirely derivative of this stuff; that relies largely on emails).

I also think some of the authorities may not be comprehensive; for example, the pre-2009 emails may have been a physical FISA search. We also know FISC has permitted the government to collect URL searches under Section 215.

But it's a damn good summary of the multiple authorities the government might use to obtain such information, by itself a superb demonstration of the many ways the government can obtain and parallel construct evidence.

The filing seems to suggest that the investigation started in fall 2009, some months after Khan's alleged co-conspirator, Ali Jalil, carried out a May 2009 suicide attack in Pakistan. If that's right, then the government obtained miscellaneous records (which is not at all surprising; these are things like immigration and PayPal records), email content, and call detail records retroactively. Alternately (Jalil was arrested in the Maldives in April 2006 and interrogated by people

presenting themselves as FBI), the government conducted all the other surveillance back to 2005 in real time, but doesn't want to show Khan's team it has. In a response to this motion, the government claims that when the surveillance of Khan began is classified.

The motion for a description of which authorities the government used to obtain particular information is still pending.

Motion to Throw Out the Emails

Here's where things get interesting.

On September 15, Khan's lawyers submitted a filing moving to throw out all the email evidence (which is the bulk of what has been shown so far and – as I said – most of what the indictment relies on). It argues the 504 emails provided in discovery – spanning from February 2005 to February 2012–lack much of the metadata detail necessary to be submitted as authenticated evidence. Some of the problems, but by no means all, stem from FBI having printed out the emails, hand-redacted them, then scanned them and sent them as “electronic production” to Khan's lawyers.

That argument is highly unlikely to get anywhere on its own, though a declaration from a forensics expert does raise real questions about the inconsistency of the metadata provided in discovery.

But the filing does pose interesting questions that – in conjunction with questions about the authorities used to investigate Khan – may be more fruitful.

First, there's FBI's computer limitations. You'll recall that one of probably several reasons why the FBI refuses to count its back door searches is because it stores traditional FISA and 702 data in the same database and claims to be unable to install tracking easily. Khan received both traditional FISA notice

(when he was arrested) and FISA 702 notice (over a year later), so both authorities are at issue in this case. The filing invokes a related problem: FBI's Data Warehouse System (DWS) – described in some detail in the Webster report on the Nidal Hasan attack publicly released in 2012, which the filing cites, and almost certainly the database that FBI says can't track back door searches – has a limited ability to maintain and process huge amounts of information.

Former FBI Director William Webster says FBI's computer systems suck (which FBI says itself, when it serves its purposes), and this filing uses that to argue the emails stored in it are therefore unreliable.

Then there are details displayed by the various fields associated with some (but not all) of the emails provided in discovery. In an appendix, Khan's lawyers provide 10 (actually, 2 appear to be duplicates) emails to demonstrate the points they make about unreliability. In addition to metadata inconsistencies, they point to redactions of several FBI fields, which may be whim or may serve to hide relevant information. Here's a summary of what they show (I've included only the last name of the non-commercial emails for privacy reasons; click to enlarge).

Email	Date	DWS	Facility	Authority
[Latsher] to reaz2000@yahoo.com	11/5/07	Yes	Redacted	FISA
[Munahaque] to reaz2000@yahoo.com	7/16/10	Yes	reaz2000@yahoo.com	Redacted
[Latsher] to reaz2000@yahoo.com (apparent dupe of 1)	11/5/07	Yes	Redacted	FISA
info@aqratravel.com to reaz2000@yahoo.com	8/27/09	No	NA	NA
[tawab] to reaz2000@yahoo.com	12/31/09	Yes	Redacted	FISA
info@aqratravel.com to reaz2000@yahoo.com (apparent dupe of 4)	8/27/09	No	NA	NA
reaz2000@yahoo.com to info@aqratravel.com (key metadata missing)	12/24/08	Yes	Redacted	FISA
reaz2000@yahoo.com to [Sohail]	8/11/09	Yes	reaz2000@yahoo.com	Redacted
reaz2000@yahoo.com to [Ideal]	3/11/08	Yes	reaz2000@yahoo.com	Redacted
reaz2000@yahoo.com to [Malaak]	11/15/08	No	NA	NA

"Facility," remember, is FISA-speak for "target." So this seems to reflect Khan's own emails coming up in FISA targeted collection with a 2008 date, before the more active investigation appears to have started (though again, that could be a search of stored email). It also seems to show Khan's emails coming up in

FISA targeted collection targeting at least two other people, one of which targeted a Yahoo to Yahoo conversation from before Yahoo complied with Protect America Act (though if this was traditional FISA, that would be unsurprising). One of the emails that seems to be from Khan-targeted collection has its authority hidden, which may be more randomness or may reflect additional authorities used to collected US person email content.

In other words, the metadata the FBI has provided and declined to provide may say some interesting things about the investigation, which used both traditional and 702 FISA.

Then there are 2 emails that appear not to have been printed out from FBI's DWS, though they do have product numbers consistent with the DWS product numbers. Because they were printed out outside of the DWS system, they lack the header information pertaining to facility and authority of the email. Of note, both emails involving Aqra Travel appear to have had some funkiness which ended up hiding key details about whom Khan was communicating with at that apparent travel agency. Maybe they're hiding that the travel agency is really in Quantico?

The filing presents these redactions as haphazard (it even cites one email turned over in illegible form early in discovery, with the authority redacted, and the same email provided later in more legible discovery, with the authority unredacted), which they may well be. But if they serve to hide that collection was targeted at someone besides Khan under other authorities, it would serve to hide the extent to which FBI built its case against Khan using back door searches on other FISA-related collection.

FBI's Problem: Timing and "Collection"

Ultimately, I think these two filings together may present two problems for the government

(though remember, the judge in this case, Michael Mosman, is a FISA Court judge who refused to recuse himself on those grounds).

First, the government has a timing problem (rather, two). As I laid out above, it looks as if this investigation into Khan started in the aftermath of Jalil's suicide attack. Perhaps the government used the phone or Western Union dragnet to identify Jalil's US associates, found Khan, and used that metadata to pull up Khan's emails with Jalil using Section 702, which then provided the basis for a FISA warrant to investigate Khan directly. But that would amount to wiretapping a dead man to read an American's emails – which would seem to qualify as reverse targeting, which is forbidden under Section 702.

Alternately, the government was wiretapping Jalil at least as early as American authorities interviewed him in 2006, and either tracked Khan through his side of those communications or they identified Khan after Jalil's attack and then pulled up already-collected emails. But if they were wiretapping Jalil communications with US persons in 2006 – including a Yahoo account – then they may have been wiretapping Jalil under Stellar Wind. Which would make Khan an aggrieved person for illegal wiretapping under FISA. Khan's lawyers have been very diligent about laying a ground work for undisclosed EO 12333 collection.

Either way, answering these questions may provide Khan a way to challenge his prosecution, which relies heavily on the emails in question.

Then there's a collection problem. As the forensics expert hired by Khan's legal team lays out, there's a really easy way to solve the authentication problems of the emails turned over to Khan.

It is my belief that much of the above noted issues regarding the lack of ability to search, sort, and even read the government provided documents

could be alleviated if the original electronic documents were provided in their native format(s) to the defense.

But not only would that reveal information the government may not want to reveal to Khan (such as where that seeming travel agency really is). But they may not be able to provide all that information, because it doesn't exist anymore and instead only exists in a database that – even the FBI agrees, when it suits the Bureau – is a dysfunctional database not up to the task of storing data with integrity.

The point is that the problems behind authenticating most of the emails (aside from the ones that may not come from FBI's database) all stem from the fact that the government has conflated "collecting" and "searching" and the means they have of accomplishing that – FBI's DWS – introduces potentially legitimate questions about authentication.

Who knows whether this effort will serve to make that distinction legally problematic or not? But it seems to target a number of the constitutional problems with the current FISA regime via the currently awful means of implementing that regime.

THE HEMISPHERE DECKS: A COMPARISON AND SOME HYPOTHESES

Last week, Dustin Slaughter published a story using a new deck of slides on the Hemisphere program, the Drug Czar program that permits agencies to access additional telecommunications analytical services to identify phones, which then gets laundered through parallel construction to hide both how those phones were

found, as well as the existence of the program itself.

It has some significant differences from the deck released by the New York Times last year.

I've tried to capture the key differences here:

	NYT	Declaration
Scope	AT&T network; CDRs for any telephone carrier that uses an AT&T switch Access to AT&T subscriber info Roaming provided, location available	"Telecom propriety" (2) though "only calls that hit the Hemisphere switches" (12) Some subscriber information unavailable (elsewhere references to "official subscriber information") Local, long distance, international, cell Temporary roaming and location provided with CDRs
Timing	1 hour response/CDRs 1 hour old	1-hour exigent; 2-5 day typical response/CDRs few hours old/CDRs 2 hours old
Customers	Fed, state, local administrative and grand jury subpoenas (mentions recent WA approval) DEA and DHS mentioned	Administrative order, CA court order, or grand jury 6 federal agencies, including FBI and US Marshals
Features	Dropped phones, additional phones, international phones, IMEI & ISEI search on AT&T network, mapping, pinging	Dropped, additional phones, international phones, temporary roaming, location
Dropped phone success rate	Candidates for the replacement phone are ranked by probability	94%
Aging	26 year old long distance and international records available in 2013 Program started in 2007	10 year old records, date unknown

The biggest difference is that the NYT deck – which must date to no earlier than June 2013 – draws only from AT&T data, whereas the Declaration deck draws from other providers as well (or rather, from switches used by other providers).

In addition, the Declaration deck seems to reflect approval for use in fewer states (given the mention of CA court orders and the recent authorization to use Hemisphere in Washington in the AT&T deck), and seems to offer fewer analytical bells and whistles.

Thus, I agree with Slaughter that his deck predates – perhaps by some time – the NYT/AT&T deck released last year. That would mean Hemisphere has lost coverage, even while it has gained new bells and whistles offered by AT&T.

While I'm not yet sure this is my theory of the origin of Hemisphere, some dates are worth noting:

From 2002 to 2006, the FBI had telecoms onsite to provide CDRs directly from their systems (the FBI submitted a great number of its requests without any paperwork). One of the services provided – by AT&T – was community of interest

tracking. Presumably they were able to track burner phones (described as dropped phones in these decks) as well.

In 2006, FBI shut down the onsite access, but retained contracts with all 3 providers (AT&T, Verizon, and probably Sprint). In 2009, one telecom – probably Verizon – declined to renew its contract for whatever the contract required.

AT&T definitely still has a contract with FBI, and in recent years, it has added more services to what it offers the FBI.

It's possible the FBI multi-provider access moved under ONCDP (the Drug Czar) in 2007 as a way to retain its authorities without attracting the attention of DOJ's excellent Inspector General (who is now investigating this in any case). Though I'm not sure that program provided the local call records the deck at least claims it could have offered. I'm not sure that program got to the telecom switches the way the deck seems to reflect. It's possible, however, that the phone dragnet in place before it was moved to Section 215 in 2006 did have that direct access to switches, and the program retained this data for some years.

The phone dragnet prior to 2006 and NSL compliance (which is what the contracts with AT&T and one other carrier purportedly provide now) are both authorized in significant part (and entirely, before 2006) through voluntary compliance, per David Kris, the NSA IG Report, and the most recent NSL report. That's a big reason why the government tried to keep this secret – to avoid any blowback on the providers.

In any case, if I'm right that the program has lost coverage (though gained AT&T's bells and whistles) in the interim, then it's probably because providers became unwilling, for a variety of reasons (and various legal decisions on location data are surely one of them) to voluntarily provide such information anymore. I suspect that voluntary compliance got even more circumscribed with the release of the first

Horizon deck last year.

Which means the government is surely scrambling to find additional authorities to coerce this continued service.

USA FREEDOM ACT'S SO-CALLED "TRANSPARENCY" PROVISIONS ENABLE ILLEGAL DOMESTIC SURVEILLANCE

I regret that I am only now taking a close look at the "transparency" provisions in Patrick Leahy's version of USA Freedom Act. They are actually designed not to provide "transparency," but to give a very misleading picture of how much spying is going on. They are also designed to permit the government to continue not knowing how much content it collects domestically under upstream and pen register orders, which is handy, because John Bates told them if they didn't know it was domestic then collecting domestic isn't illegal.

In this post, I've laid out the section of the bill that mandates reporting from ODNI, with my comments interspersed along with what the "transparency" report Clapper did this year showed.

(b) MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—

(1) IN GENERAL.—Except as provided in subsection (e), the Director of National Intelligence shall annually make publicly available on an Internet Web

site a report that identifies, for the preceding 12-month period—

This language basically requires the DNI to post a report on I Con the Record every year. But subsection (e) provides a number of outs.

Individual US Person FISA Orders

(A) the total number of orders issued pursuant to titles I and III and sections 703 and 704 and a good faith estimate of the number of targets of such orders;

This language requires DNI to describe, in bulk, how many individual US persons are targeted in a given year (there were 1,767 orders and 1,144 estimated targets last year). But it only requires DNI to give a “good faith estimate” of these numbers (and that’s what they’re listed as in ODNI’s report from last year)! If there’s one thing DNI should be able to give a rock-solid number for, it’s individual USP targets. But ... apparently that’s not the case.



Section 702 Orders

(B) the total number of orders issued pursuant to section 702 and a good faith estimate of—

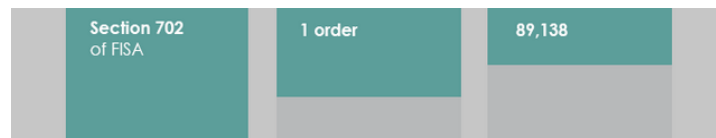
(i) the number of targets of such orders;

(ii) the number of individuals whose communications were collected pursuant

to such orders;

(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection;

This language requires DNI to provide an estimate of the number of targets of Section 702 which includes both upstream and PRISM production. Last year, this was one order (ODNI doesn't tell us, but there were at least 3 certificates –Counterterrorism, Counterproliferation, and Foreign Government) affecting 89,138 targets.



The new reporting requires the government to come up with some estimate of how many communications are collected, as well as how many are located inside the US.

Except DNI is permitted to issue a certification saying that there are operational reasons why he can't provide that last bit – how many are in the US. Thus, 4 years after refusing to tell John Bates how many Americans' communications NSA was sucking up in upstream collection, Clapper is now getting the right to continue to refuse to provide that ratified by Congress. And remember – Bates also said that if the government didn't know it was collecting that content domestically, then it wasn't really in violation of 50 USC 1809(a). So by ensuring that it doesn't have to count this, Clapper is ensuring that he can continue to conduct illegal domestic surveillance.

Don't worry though. The bill includes language that says, even though this provision permits the government to continue conducting illegal domestic collection, "Nothing in this section affects the lawfulness or unlawfulness of any

government surveillance activities described herein. ”

Back Door Searches

(iv) the number of search terms that included information concerning a United States person that were used to query any database of the contents of electronic communications or wire communications obtained through the use of an order issued pursuant to section 702; and

(v) the number of search queries initiated by an officer, employee, or agent of the United States whose search terms included information concerning a United States person in any database of noncontents information relating to electronic communications or wire communications that were obtained through the use of an order issued pursuant to section 702;

This language counts back door searches.

But later in the bill, the FBI – which we know does the bulk of these back door searches – is exempted from all of this reporting. As I noted in this post, effectively the Senate is saying it’s no big deal of FBI doesn’t track how many warrantless searches of US person content it does, even of people against whom the FBI has no evidence of wrongdoing.

In addition, note that odd limit to (v). DNI only has to report metadata searches “initiated by an officer, employee, or agent” of the United States. That would seem to exempt any back door metadata searches by foreign governments (it might also exempt contractors, but they should be included as “agents” of the US). Which, given that CIA doesn’t currently count its metadata searches, and given that CIA conducts a bunch of metadata searches on behalf of other entities,

leads me to suspect that CIA may be doing metadata searches “initiated” by foreign governments. But that’s a guess. One way or another, though, this clause was written to not count some of these metadata searches. [Update: On reflection, that language may be designed to avoid counting automated processes as searches – if they’re initiated by a robot rather than an employee they’re not counted!]

Pen Register Orders

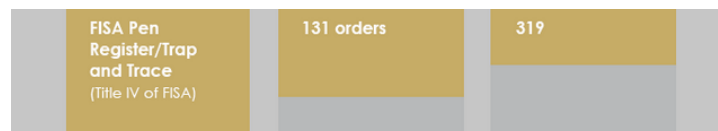
C) the total number of orders issued pursuant to title IV and a good faith estimate of–

(i) the number of targets of such orders;

(ii) the number of individuals whose communications were collected pursuant to such orders; and

(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection;

This language counts how many Pen Register orders the government obtains, how many individuals get sucked up, and how many are in the US, both of which are additions on what ODNI reported this year.



But that last bit – counting people in the US – is again a permissible exemption under the bill. Which is, as you’ll recall, the other way NSA has been known to engage in illegal domestic content collection. The only known bulk pen register is currently run by FBI, but in any case, the exemption has the same effect, of

permitting the government from ever having to admit that it is breaking the law.

Traditional Section 215 Collection

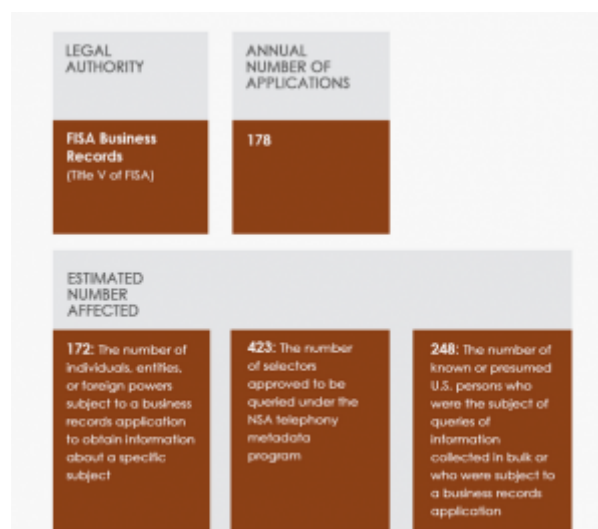
(D) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—

(i) the number of targets of such orders;

(ii) the number of individuals whose communications were collected pursuant to such orders; and

(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection;

This requires DNI to report on traditional Section 215 orders, but the entire requirement is a joke on two counts.



First, note that, for a reporting requirement for a law permitting the government to collect “tangible things,” it only requires individualized reporting for “communications.”

"Individuals whose communications were collected" are specifically defined as only involving phone calls and electronic communications.

So this "transparency" bill will not count how many individuals have their financial records, beauty supply purchases, gun purchases, pressure cooker purchases, medical records, money transfers, or other things sucked up, much of which we know to be done under this bill. And this is particularly important, because the law still permits bulk collection of these things. Thus, this "transparency" report creates the illusion that far less collection is done under Section 215 than actually is, it creates the illusion that bulk collection is not going on when it is.

But it gets worse!

After having limited the individualized reporting solely to communications, the bill also exempts FBI from (iii). And that's important because we know the majority of Section 215 orders are being used to order Internet companies to provide something that the government failed to obtain using NSLs. Those orders are almost certainly minimized, meaning they involve significant bulk either in terms of people sucked up or in terms of sensitive First Amendment materials (which might be the case for URL searches). So while the bill will show how many people have their communications collected, the reports will wrongly suggest Americans' communications aren't being sucked up.

So the traditional 215 reporting will show the orders and targets of the orders, but will hide how many individuals are having their non-communications records sucked up, and how many Americans communications records the FBI is sucking up. This report will give an unbelievably deceptive picture of how Section 215 is being used.

Newfangled Section 215 Reporting

(E) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—

(i) the number of targets of such orders;

(ii) the number of individuals whose communications were collected pursuant to such orders;

(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection; and

(iv) the number of search terms that included information concerning a United States person that were used to query any database of call detail records obtained through the use of such orders; and

This is the reporting on the new Call Detail Record provision. It purports to show how many orders are issued, the number of targets, the number of individuals collected, and the number of Americans implicated, either by having their communications collected or using information from a US person to conduct the query.

But ... you guessed it! There's another exemption for the FBI, covering the two US person provisions.

Now, I assume that, given this provision will no longer require the ingestion of all the call records of all Americans every day, this collection may actually go back to the FBI, where it belongs. If that's the case, then it

means the CDR “transparency” report will, again, provide a completely misleading impression that no Americans are being sucked up.

National Security Letters

(F) the total number of national security letters issued and the number of requests for information contained within such national security letters.

~~This bill prohibits bulk collection!!!! its supporters claim. But with NSLs — a collection conducted with no oversight from courts — the bill doesn’t require reporting of the total people affected. (Current reporting hides bulk collection with NSLs of what are basically phone books by not requiring those to be broken out by US person.) This is, admittedly, way down on my list of things that worry me about these “transparency” provisions. But still, another indication of how seriously this bill takes “transparency.”~~

Update, 10/4: This is incorrect. A different provision requires reporting on this, which is in fact slightly better than what we currently get.

The Fine Print and Other Loopholes

(2) BASIS FOR REASONABLE BELIEF INDIVIDUAL IS LOCATED IN UNITED STATES.—A phone number registered in the United States may provide the basis for a reasonable belief that the individual using the phone number is located in the United States at the time of collection.

I’m not sure whether this is the intent, but I

believe this language provides DNI another way to not report when it collects Internet data in the US – because an IP address located in the US is not considered a reasonable basis to believe the person using that IP address is located in the US. So it may well make the Internet reporting even more inaccurate.

(c) DISCRETIONARY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—The Director of National Intelligence may annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period—

(1) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to titles I and III and sections 703 and 704 reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States;

(2) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to section 702 reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States;

(3) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to title IV reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States;

(4) a good faith estimate of the number of individuals whose communications were

collected pursuant to orders issued pursuant to applications made under section 501(b)(2)(B) reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States; and

(5) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to applications made under section 501(b)(2)(C) reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States.

This discretionary reporting is all designed to allow James Clapper to come out every year and say, “sure, we’ve got all your Gmail in a server somewhere, but don’t worry, we didn’t look at it.” Note that it doesn’t talk about electronic access, just human access, and doesn’t talk about foreign person access.

(d) TIMING.—The annual reports required by subsections (a) and (b) and permitted by subsection (c) shall be made publicly available during April of each year and include information relating to the previous year.

The timing of reports will match current timing.

(e) EXCEPTIONS.—

(1) REPORTING BY UNIQUE IDENTIFIER.—If it is not practicable to report the good faith estimates required by subsection (b) and permitted by subsection (c) in terms of individuals, the good faith estimates may be counted in terms of unique identifiers, including names, account names or numbers, addresses, or

telephone or instrument numbers.

This is, I think, a totally innocuous provision permitting DNI to not have to run its correlations tool against this reporting.

(2) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under clauses (ii) or (iii) of each of subparagraphs (B), (C), (D), and (E) of paragraph (1) of subsection (b) or permitted to be reported in subsection (c), is fewer than 500, it shall exclusively be expressed as a numerical range of 'fewer than 500' and shall not be expressed as an individual number.

This says that DNI can use 500 rather than provide a specific number for the individualized reports. Note that's worse than what they did this year on Section 215.

(3) FEDERAL BUREAU OF INVESTIGATION.—Subparagraphs (B)(iv), (B)(v), (D)(iii), (E)(iii), and (E)(iv) of paragraph (1) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation.

As I noted, the FBI has exemptions for things that the FBI does the bulk of. There is another grave problem with this exemption, which I'll get to in another post.

(4) CERTIFICATION.—

(A) IN GENERAL.—If the Director of National Intelligence concludes that a good faith estimate required to be reported under subparagraph (B)(iii) or (C)(iii) of paragraph (1) of subsection (b) cannot be determined accurately, including through the use of statistical sampling, the Director shall—

(i) certify that conclusion in writing to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate; and

(ii) make such certification publicly available on an Internet Web site.

(B) CONTENT.—

(i) IN GENERAL.—The certification described in subparagraph (A) shall state with specificity any operational, national security, or other reasons why the Director of National Intelligence has reached the conclusion described in subparagraph (A).

This is the language that permits DNI to not count the stuff that would be illegal if he counted it. Also note – one of my favorite bits! – House Judiciary does not get this report (the bill fixes non-reporting to HJC on most other provisions).

Remarkably, it permits DNI to provide “national security” reasons why he can’t count this accurately. Such certification will say something like, “If I count this stuff, it then becomes illegal, and I’ll no longer be able to illegally collect US person content in the US anymore, which will be bad for national security, so I certify that I can’t count it.”

GOOD FAITH ESTIMATES OF CERTAIN INDIVIDUALS WHOSE COMMUNICATIONS WERE COLLECTED UNDER ORDERS ISSUED UNDER SECTION 702.—A certification described in subparagraph (A) relating to a good faith estimate required to be reported under subsection (b)(1)(B)(iii) may include the information annually reported pursuant to section 702(l)(3)(A).

‘(iii) GOOD FAITH ESTIMATES OF CERTAIN INDIVIDUALS WHOSE COMMUNICATIONS WERE COLLECTED UNDER ORDERS ISSUED UNDER TITLE IV.—If the Director of National Intelligence determines that a good faith estimate required to be reported under subsection (b)(1)(C)(iii) cannot be determined accurately as that estimate pertains to electronic communications, but can be determined accurately for wire communications, the Director shall make the certification described in subparagraph (A) with respect to electronic communications and shall also report the good faith estimate with respect to wire communications.

This says that DNI may report only the phone conversations collected under 702, but not the wire communications – the stuff that’s illegal.

(C) FORM.—A certification described in subparagraph (A) shall be prepared in unclassified form, but may contain a classified annex.

(D) TIMING.—If the Director of National Intelligence continues to conclude that the good faith estimates described in this paragraph cannot be determined accurately, the Director shall annually submit a certification in accordance with this paragraph.

Hey! At least we’ll know that DNI refuses to count its illegal domestic collection. Every year he’ll write a note to Congress saying, “I still refuse to count how many people get sucked up under 702,” with the classified bit explaining that if he counted it, then it’d be illegal.

HOSPITAL HERO JACK GOLDSMITH, THE DESTROYER OF THE INTERNET DRAGNET, AUTHORIZED THE INTERNET DRAGNET

As I noted earlier, I think the re-release of Jack Goldsmith's May 6, 2004 OLC memo authorizing Stellar Wind is meant to warn Congress that the Executive does not believe it needs any Congressional authorization to spy on every American – just in time for the USA Freedom Act debate in the Senate. This is exactly parallel to similar provocations during the Protect America Act debate. In the past, such provocations led Congress to capitulate to Executive branch demands to tailor the program to their wishes.

That earlier post, however, implied that this warning pertains primarily to the phone dragnet.

It doesn't. The warning also applies to the Internet dragnet (and I suspect that stories about the heroic hospital heroes shutting down the Internet dragnet have been dramatically overblown).

One of the very few things – aside from the name STELLAR WIND, over and over, as well as references to content collection that could have been released after President Bush admitted to that part of the program in 2005, and the title Secretary of Defense – that has been newly revealed is this bit of the Table of Contents (here's the previous release for comparison).

III. Telephony Dialing-Type Meta Data Collection – Statutory Analysis	81
A. [REDACTED]	83
B. [REDACTED]	86
C. [REDACTED]	89
IV. [REDACTED]	96
[REDACTED]	96
[REDACTED]	98
[REDACTED]	99
[REDACTED]	100
V. STELLAR WIND Under the Fourth Amendment	100
A. STELLAR WIND Content Interceptions Are Reasonable Under Balancing-of-Interests Analysis ..	101
B. Acquisition of Meta Data Does Not Implicate the Fourth Amendment	106

It shows that the memo discusses content, discusses telephony metadata, discusses something else, then concludes that content and metadata are both kosher under the Fourth Amendment. That already makes it clear that part IV is about metadata. The last sentence of the first full paragraph on page 19 does, too. Page 7 makes it clear that Fourth Amendment analysis applies to “both telephony and e-mail.” Much later in the memo, it becomes clear this section – pages 96 to 100 – deals with Internet metadata.

In fact, the *only* substantive newly unredacted parts of the memo appear on 101 (PDF 69) and then from 106 to 108.

All of this new information makes it clear that Goldsmith asserted that *Smith v. Maryland* applied for metadata – and applied to both phone and Internet metadata. Remarkably, in that analysis, the government keeps at least one paragraph addressing phone metadata hidden, but reveals the analysis at 106-7 (PDF 74-75) that applies to Internet. (Goldsmith’s claim that Internet users can get providers to turn off spam, at the bottom of 107, is particularly nice.)

In perhaps the most interesting newly released passage (out of the roughly 5 pages that got newly released!), Goldsmith absolves himself of examining what procedures the government was using in its “metadata” collection.

As for meta data collection, as explained below, we conclude that under the Supreme Court’s decision in *Smith v.*

Maryland, 442 U.S. 735 (1979), the interception of the routing information for both telephone calls and e-mails does not implicate any Fourth Amendment interests.⁸⁵

85 Although this memorandum evaluates the STELLAR WIND program under the Fourth Amendment, we do not here analyze the specific procedures followed by the NSA in implementing the program.
(101/PDF 69)

I find this utterly damning, given that we know that, for the following 5 years, the government would lie to FISC about whether their “metadata” contained content. Even the OLC opinion built in the Executive’s ability to collect content in the guise of metadata!

In any case, what is clear – again, just in time to impact the debate over USA Freedom, for which prospective call record collection might or might not be limited to telephone content – is that rather than legally shutting down the Internet dragnet in 2004, Jack Goldsmith authorized it.

And that authorization remains in place, telling the Executive it can collect Internet (and phone) “metadata” whether or not FISC or Congress rubberstamps it doing so. Not only that, but telling the Executive this analysis holds regardless of how inadequate their procedures are in implementing this program to ensure that no content gets swept up in the guise of metadata (which of course is precisely what occurred).

So the Administration, in releasing this “newly unredacted” memo did one thing. Tell Congress it will continue to collect phone and Internet “metadata” on its own terms, regardless of what Congress does.

Only one thing could alter this analysis of course: if the Courts decide that *Smith v. Maryland* doesn’t actually permit the government

to collect all metadata, plus some content-as-metadata, in the country, if they say the Executive can't actually collect "everything there is to know about everybody and have it all in one big government cloud," as 2nd Circuit Judge Gerard Lynch described the implications of what we now know to be Goldsmith's logic on Tuesday. But the courts are going to stop analyzing this question as soon as Congress passes USA Freedom Act. Moreover, the last check on the program – the unwillingness of providers to break the law – will be removed by the broad immunity provision included in the bill.

Not only didn't Jack Goldsmith heroically legally shut down the Internet dragnet in 2004 (clearly President Bush did make several modifications; we just still don't know what those are). But he provided a tool that is likely proving remarkably valuable as the Executive gets Congress and privacy NGOs to finish signing off on their broad authority.

The hospital heroes may have temporarily halted the conduct of the Internet dragnet – even while telling Colleen Kollar-Kotelly she had to rubber stamp ignoring the letter of the law because Congress couldn't know about the dragnet – but they didn't shut it down. Here it is, legally still operating, just in time to use as a cudgel with Congress.

Update: One other thing other reporting on this is missing – and not for the first time – is that whatever change they made to the Internet dragnet, it was by no means the only change after the hospital confrontation. They also took Iraqi targeting out (in some way). And there was a later April 2 modification that appears to have nothing to do with NSA at all (I have my theories about this, but they're still theories). So it is too simple to say the hospital confrontation was exclusively about the Internet dragnet – the public record already makes clear that's not the case.

TWO EXPLANATIONS FOR CONFUSION ABOUT US ISIS MEMBERS: ASSOCIATIONAL CLAIMS AND WATCHLISTING PROCEDURES

Eli Lake has a piece trying to explain the big disparities between claimed numbers of Americans who have joined ISIS.

One might think that a government that secretly collected everyone's cellphone records would be able to find out which Americans have joined ISIS. But actually that task is much harder than it would appear.

On Wednesday, Secretary of Defense Chuck Hagel told CNN more than 100 Americans have pledged themselves to the group that declared itself a Caliphate in June after conquering Iraq's second-largest city. Hagel added, "There may be more, we don't know." On Thursday, a Pentagon spokesman walked back Hagel's remarks, [saying](#) the United States believes there are "maybe a dozen" Americans who have joined ISIS.

"We don't know what we don't know," a U.S. intelligence official told The Daily Beast when asked if there were more than 12 Americans in ISIS. "We have some identifying information on some of the Americans, it may not be their name but we have enough information. That said, we readily acknowledge that that number is probably low and there are others we don't know about."

"I think 12 is probably low only because there is always stuff we don't know," said Andrew Liepman, who left his post as the deputy director of the National Counterterrorism Center (NCTC) in 2012 and is now a senior policy analyst at the Rand Corporation. "I would not say that number is hugely low, but we always have to remember what we don't know."

But at least some of these discrepancies are actually quite easy to explain.

First, Lake jokes about the NSA's dragnet. But that is actually one explanation for the larger numbers: in FISC documents, it is clear NSA treats association as transitive, meaning that an association with someone who is known to be associated with a group is itself, in many cases, considered evidence of association with the group. And some of this analysis is not going to go beyond metadata analysis (meaning NSA may not get around to reading the content to confirm the association unless the metadata patterns suggest some reason to prioritize the captured communication).

Thus, for any Americans who are in email or phone contact with a known or suspected member of ISIS, NSA likely considers them to be associated with ISIS. And remember, NSA's collection of email and phone records overseas is almost certainly more extensive than their collection here, meaning those contact chains will be more exhaustive.

In addition, we know that the government considers traveling to an area of terrorist activity to be reasonable suspicion that someone is a known or suspected terrorist. The watchlist guidelines list just that as one behavioral indicator for being watchlisted as a known or suspected terrorist (see page 35).

3.9.4 Travel for no known lawful or legitimate purpose to a locus of
TERRORIST ACTIVITY.

This means that any Americans who have traveled to Syria or Iraq are likely classified, by default, as terrorists. And many of those may have traveled for entirely different reasons (like freelance journalism).

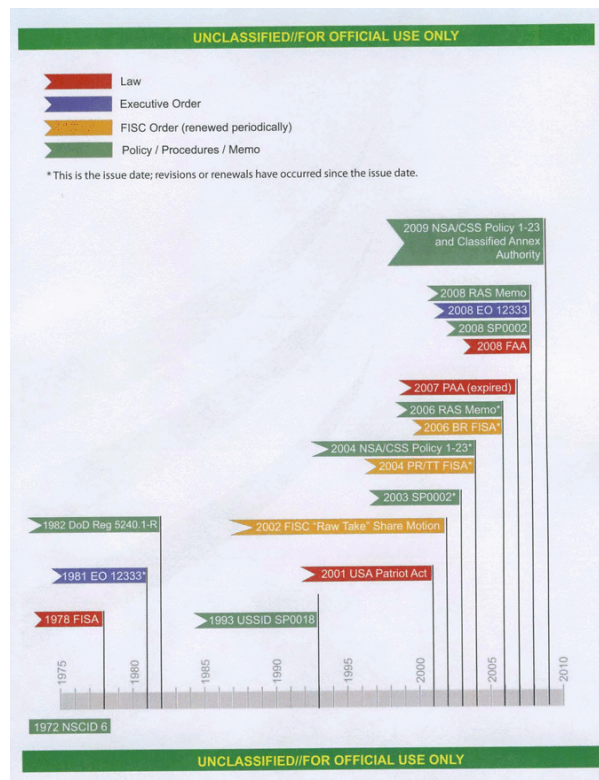
That the Pentagon responded the way it did to Chuck Hagel's fear-mongering is itself tacit admission that the government's means of tracking terrorist affiliation sweep far wider than actual terrorist affiliation actually does. All Americans who have communicated with ISIS or traveled to Syria may not even want to join ISIS, and not all that want to will succeed in doing so. But NSA and NCTC are going to track everyone who might want to join, because that's the best way to keep us safe.

Of course, that means the numbers can be used as Hagel used them, to fearmonger about the possible rather than the actual threat of American ISIS members.

All the more reason to make these watchlisting details public!

**MISSING FROM THE EO
12333 DISCUSSION: ITS
CLASSIFIED ANNEX
MICHAEL HAYDEN
REVISED ON MARCH 11,
2004**

I
recomm
end
this
ArsTec
hnica
backgr
ound
piece
on EO
12333.
It
descri
bes
how
Ronnie
Reagan
issued
EO



12333 to loosen the intelligence rules imposed by Jimmy Carter (with links to key historical documents). It includes interviews with the NSA whistleblowers describing how George Bush authorized the collection of telecom data from circuits focused on the US under the guise of EO 12333, calling the bulk of the US person data collected "incidental." And it describes how Bush and Obama have continued using EO 12333 as a loophole to obtain US person data.

But there's a key part of the story Ars misses, which I started to lay out here. As this graphic notes, the NSA is governed by a set of interlocking authorities and laws. The precedence of those authorities and laws is not terribly clear – and NSA's own training programs don't make them any more clear. Bush's revision to EO 12333 played on that interlocking confusion.

Perhaps most alarming, however, the NSA continued to use a classified annex to EO 12333 written by Michael Hayden the day he reauthorized the illegal wiretap program at least until recent years – and possibly still. And that classified annex asserts an authority to wiretap Americans on the Attorney General's

authorization for periods of up to 90 days, and wiretap “about” collection based solely on NSA Director authority.

Among the documents released to ACLU and EFF via FOIA was an undated “Core Intelligence Oversight Training” program that consists of nothing more than printouts of the authorities governing NSA activities (as I noted in this post, with one exception, the NSA training programs we’ve seen are unbelievably horrible from a training efficacy standpoint). It includes, in part, EO 12333, DOD 5240.1-R, and NSA/CSS Policy 1-23 (that is, several of the authorities NSA considers among its signature authorities). As part of a 2009 issuance of the latter document (starting on page 110), the training documents also include the classified annex to EO 12333 (starting on page 118). And although both documents are part of that 2009 issuance (which incorporated language reflecting the FISA Amendments Act), they are dated March 11, 2004 – the day after the hospital confrontation, when the Bush Administration continued its illegal wiretap program without DOJ sanction – and signed by then DIRNSA Michael Hayden.

That is, as part of the FOIA response to ACLU and EFF, DOJ revealed how it was secretly applying EO 12333 at least as recently as 2009.

And that secret application of EO 12333 includes two provisions that illustrate how the government was abusing EO 12333, even in the face of revisions to FISA. They include provisions permitting the wiretapping of Americans for 90-day periods based on AG certification, and the wiretapping of “about” communications for apparently unlimited periods based on DIRNSA certification. (see page 123)

Here’s the AG-certified 90-day provision.

(4) with specific prior approval by the Attorney General based on a finding by the Attorney General that there is probable cause to believe the United States person is an agent of a foreign

power and that the purpose of the interception or selection is to collect significant foreign intelligence. Such approvals shall be limited to a period of time not to exceed ninety days for individuals and one year for entities.

The illegal wiretap program operated on 45-day authorizations from the AG. We don't know from this what changes Hayden made the day after DOJ refused to reauthorize the program, but if Hayden changed it to 90 days, it effectively extended the previous authorization for another period.

And here's the part of the "about" collection that is not redacted.

(b) Communications of, or concerning (1) [redacted] of a foreign power, or powers, as defined in Section 101 (a) (1) – (3) of FISA or (2) [redacted] may be intercepted intentionally, or selected deliberately (through the use of a selection term or otherwise), upon certification in writing by the Director, NSA to the Attorney General. Such certification shall take the form of the Certification Notice appended thereto. An information copy shall be forwarded to the Deputy Secretary of Defense. Collection may commence upon the Director, NSA's certification. In addition, the Director, NSA shall advise the Attorney General and the Deputy Secretary of Defense on an annual basis of all such collection.

This "about" collection is ostensibly not targeted at US persons, but we know from the problems NSA confessed to in the 2011 702 upstream program that "about" collection ensnares a good deal of US person data – so much so NSA could not or would not count it when John Bates asked them to.

At least 5 years after the hospital confrontation and 2 years after Congress purportedly passed laws addressing the underlying issue, NSA's own secret interpretation of how it implemented E.O. 12333 said it could continue to do the same domestic wiretapping, authorized by either the AG (for wiretapping targeting US persons for up to 90-day periods) or the DIRNSA (for wiretapping targeting communications "about" foreign powers).

The Bush Administration explicitly argued it was not bound by FISA – the law that should govern both these activities. Did the Obama Administration continue that policy?

October 20, 2014 update: As far as I can tell, Hayden's version of the classified annex was identical to the annex as issued in 1988, released here (there are different redactions in the release). Given this language, it appears to reflect a reversion to the earlier policy, overriding Clinton-era changes.

This Policy 1-23 supersedes Directive 10-30, dated 20 September 1990, and Change One thereto, dated June 1998. The Associate Director for Policy endorsed an administrative update, effective 27 December 2007 to make minor adjustments to this policy. This 29 May 2009 administrative update includes changes due to the FISA Amendments Act of 2008 and in core training requirements.

SPCMA AND ICREACH

Within weeks of Michael Mukasey's confirmation as Attorney General in November 2007, Assistant Attorney General Ken Wainstein started pitching him to weaken protections then in place for US person metadata collected overseas; Mukasey did

so, under an authority that would come to be known as SPCMA, on January 3, 2008.

In 2007, Wainstein explained the need to start including US person data in its metadata analysis, in part, because CIA wanted to get to the data – and had been trying to get to it since 2004.

(3) The Central Intelligence Agency's (CIA) Interest in Conducting Similar Communications Metadata Analysis. On July 20, 2004 [days after CIA had helped NSA get the PRTT dragnet approved], the General Counsel of CIA wrote to the General Counsel of NSA and to the Counsel for Intelligence Policy asking that CIA receive from NSA United States communications metadata that NSA does not currently provide to CIA. The letter from CIA is attached at Tab C. Although the proposed Supplemental Procedures do not directly address the CIA's request, they do resolve a significant legal obstacle to the dissemination of this metadata from NSA to CIA. (S//SII/NF)

Wainstein also noted other DOD entities might access the information.

That's important background to the Intercept's latest on ICREACH, data sharing middleware that permits other intelligence agencies to access NSA's metadata directly – and probably goes some way to answer Jennifer Granick's questions about the story.

As the documents released by the Intercept make clear, ICREACH arose out of an effort to solve a data sharing effort (though I suspect it is partly an effort to return to access available under Bush's illegal program, in addition to expanding it). A CIA platform, PROTON, had been the common platform for information sharing in the IC. NSA was already providing 30% of the data, but could not provide some of the types of data it had (such as email metadata) and could not adequately protect some of it. Nevertheless, CIA was making repeated requests for more data. So starting in 2005, NSA proposed ICREACH, a middleware platform that would provide access to

both other IC Agencies as well as 2nd parties (Five Eyes members). By June 2007, NSA was piloting the program.

Right in that same time period, NSA's Acting General Counsel Vito Potenza, Acting OLC head Steven Bradbury, and Wainstein started changing the rules on contact chaining including US person metadata. They did so through some word games that gave the data a legal virgin birth as stored data that was therefore exempt from DOD's existing rules defining the interception or selection of a communication.

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

See this post for more on this amazing legal virgin birth.

Significantly, they would define metadata the same way ICREACH did (page 4), deeming certain login information to be metadata rather than content.

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

It would take several years to roll out SPCMA (remember, that's the authority to chain on US person data, as distinct from the sharing platform); a pilot started in NSA's biggest analytical unit in 2009. When it did, NSA made it clear that personnel could access this data to conduct analysis, but that existing dissemination rules remained the same (which is consistent with the 2006-2008 proposed activity).

Additionally, the analyst must remain cognizant of minimization procedures associated with retention and dissemination of US person information. SPCMA covers *analytic* procedures and does not affect existing procedures for collection, retention or dissemination of US person information. [emphasis original]

Accessing data in a database to do analysis, NSA appears to have argued, was different than disseminating it (which is a really convenient stance when you're giving access to other agencies and trying to hide the use of such analysis).

Of course, the pitch to Mukasey only nodded to direct access to this data by CIA (and through them and PROTON, the rest of the IC) and other parts of DOD. In what we've seen in yesterday's documents from the Intercept and earlier documents on SPCMA, NSA wasn't highlighting that CIA would also get direct access to this data under the new SPCMA authority, and therefore the data would be disseminated via analysis outside the NSA. (Note, I don't think SPCMA data is the only place NSA uses this gimmick, and as I suggested I think it dates back at least to the illegal dragnet.)

In response to yesterday's Intercept story, Jennifer Granick suggested that by defining this metadata as something other than communication, it allows the NSA to bypass its minimization procedures.

The same is true of the USSID18 procedures. If the IC excludes unshared

stored data and other user information from the definition of communications, no minimization rules at all apply to protect American privacy with regard to metadata NSA collects, either under 12333 or section 702.

[snip]

NSA may nevertheless call this “minimized”, in that the minimization rules, which require nothing to be done, have been applied to the data in question. But the data would not be “minimized” in that it would not be redacted, withheld, or deleted.

Given what we’ve seen in SPCMA – the authority permitting the analysis of expansively defined metadata to include US person data – she’s partly right – that the NSA has defined this metadata as something other than communication “selection” – but partly missing one of NSA’s gimmicks – that NSA distinguishes “analysis” from “dissemination.”

And if a bunch of agencies can access this data directly, then it sort of makes the word “dissemination” meaningless.

June 2004: DCID 8/1 mandates that all IC agencies share data as soon as it might be comprehensible.

July 20, 2004: Scott Muller writes NSA GC (Potenza?) and OIPR Counsel, asking for US person metadata.

March 10, 2005: CIA requests additional data for PROTON

May 26, 2005: NSA/CSS Policy 1-9: Information Sharing implements DCID 1/8

July 6, 2005: Recommendation NSA make PROTON available on GLOBALREACH; this would become ICREACH

September 28, 2006: NSA Acting General Counsel first asks James Baker to permit contact chaining through US person data overseas

FY 2007: Rollout and training of ICREACH

FY 2008: Add second party and PROTON brokers to ICREACH

June 2007: ICREACH pilot begins

~July 2009: SPCMA pilot

January 2011: SPCMA expands across NSA

BEHOLD, JOHN BRENNAN'S SCARY MEMO!

I've
been
writin
g for
a long
time
about
the
"Scary
Memos"



the government used to justify its dragnet.

As the Joint IG Report described, they started in tandem with George Bush's illegal wiretap program, and were written before each 45-day reauthorization to argue the threat to the US was serious enough to dismiss any Fourth Amendment concerns that the President was wiretapping Americans domestically.

Jack Goldsmith relied on one for his May 6, 2004 memo reauthorizing some – but not all – of the dragnet.

Yesterday, James Clapper's office released the Scary Memo included in the FISA Court application to authorize the Internet dragnet just two months later, on July 14, 2004.

ODNI calls it the Tenet Declaration – indeed it is signed by him (which, given that he left government on July 11, 2004 and that final FISC applications tend to be submitted days before their approval, may suggest signing this Scary Memo was among the very last things he did as CIA Director).

Yet the Memo would have been written by the Terrorist Threat Integration Center, then headed by John Brennan.

Much of the Scary Memo describes a “possible imminent threat” that DOJ plans to counter by,

seeking authority from this Court [redacted] to install and use pen register and trap and trace devices to support FBI investigations to identify [redacted], in the United States and abroad, by obtaining the metadata regarding their electronic communications.

There is no mention of NSA. There is no mention that the program operated without legal basis for the previous 2.5 years. And there’s a very curious redaction after “this Court;” perhaps CIA also made a show of having the President authorize it, so as to sustain a claim that all this could be conducted exclusively on Presidential authority?

After dropping mention of WMD – anthrax! fissile material! chemical weapons! – the Scary Memo admits it has no real details about this “possible imminent threat.”

[W]e have no specific information regarding the exact times, targets, or tactics for those planned attacks, we have gathered and continue to gather intelligence that leads us to believe that the next terrorist attack or attacks on US soil could be imminent.

[snip]

Reporting [redacted] does not provide

specific information on the targets to be hit or methods to be used in the US attack or attacks.

But based on “detainee statements and [redacted] public statements since 9/11,” the Scary Memo lays out, CIA believes al Qaeda (curiously, sometimes they redact al Qaeda, sometimes they don’t) wants to target symbols of US power that would negatively impact the US economy and cause mass casualties and spread fear.

It took an “intelligence” agency to come up with that.

Based on that “intelligence,” it appears, but not on any solid evidence, CIA concludes that the Presidential conventions would make juicy targets for al Qaeda.

Attacks against or in the host cities for the Democratic and Republican Party conventions would be especially attractive to [redacted].

And because of that – because CIA’s “intelligence” has decided a terrorist group likes to launch attacks that cause terror and therefore must be targeting the Presidential conventions – the FBI (though of course it’s really the NSA) needs to hunt out “sleeper cells.”

Identifying and disrupting the North American-based cells involved in tactical planning offers the most direct path to stopping an attack or attacks against the US homeland. Numerous credible intelligence reports since 9/11 indicate [redacted] has “sleepers” in North America. We judge that these “sleepers” have been in North American, and the US in general, for much of the past two years. We base our judgment, in part, [redacted] as well as on information [redacted] that [redacted] had operatives here.

Before we get to what led CIA to suggest the US was targeted, step back and look at this intelligence for a moment. This report mentions detainee reporting twice. It redacts the name of what are probably detainees in several places. Indeed, several of the claims in this report appear to match those from the exactly contemporaneous document CIA did on Khalid Sheikh Mohammed to justify its torture program, thus must come from him.

Yet, over a year after KSM had been allegedly rendered completely cooperative via waterboarding, CIA still did not know the answer to a question that KSM was probably one of the only people alive who could answer.

We continue to investigate whether the August 2001 arrest of Zacarias Moussaoui may have accelerated the timetable for the 9/11 attacks because he knew of al-Qa'ida's intention to use commercial aircraft as weapons.

Nevertheless, they believed KSM was being totally straight up and forthcoming.

Note, too, the CIA relied on claims of sleeper cells that were then two years old, dating back to the time they were torturing Abu Zubaydah, whom we know did give "intelligence" about sleeper cells.

To be sure, we know CIA's claims of a "possible imminent threat" in the US do not derive exclusively from CIA's earlier torture (though CIA had claimed, just months earlier, that their best intelligence came from that source for the Inspector General's report).

Less than 3 weeks after this Scary Memo was written, we'd begin to see public notice of this "possible imminent threat," when Tom Ridge raised the threat level on August 1, 2004 because of an election year plot, purportedly in response to the capture of Muhammad Naeem Noor Khan in Pakistan on July 13 (which could only have been included in "the Tenet declaration" if

Khan were secretly arrested and flipped earlier, because Tenet was no longer CIA Director on July 13). But what little basis the election year plot had in any reality dated back to the December 2003 British arrest and beating of Khan's cousin, Babar Ahmed, which would lead to both Khan's eventual capture as well as the British surveillance of Dhiren Barot as early as June 10 and the latter's premature arrest on August 3. KSM's nephew, Musaad Aruchi, was also handed over by Pakistan to CIA on June 12; best as I know, he remains among those permanently disappeared in CIA's torture program. This would also lead to a new round of torture memos reauthorizing everything that had been approved in the August 1, 2002 Bybee Memo plus some.

The claims the US was a target derive, based on the reporting in the NYT, from Dhiren Barot. Barot apparently did want to launch a terrorist attack. Both KSM and Hambali had identified Barot during interrogations in 2003, and he had scouted out attack sites in the US in 2000 and 2001. But his active plots in 2004 were all focused on the UK. In 2007 the Brits reduced his sentence because his plots weren't really all that active or realistic.

Which is to say this election plot – the Scary Plot that drives the Scary Memo that provided the excuse for rolling out (or rather, giving judicial approval for continuing) an Internet dragnet that would one day encompass all Americans – arose in significant part from 2003 torture-influenced interrogations that led to the real world detention of men who had contemplated attacking the US in 2000, but by 2004 were aspirationally plotting to attack the UK, not the US, as well as men who may have been plotting in Pakistan but were not in the US.

That, plus vague references to claims that surely were torture derived, is what John Brennan appears to have laid out in his case for legally justifying a US dragnet.

You see, it's actually John Brennan's dragnet – it all goes back to his Scary Memo – and his

role in it is presumably one of the reasons he doesn't want us to know how many lies went into the CIA torture program.

Brennan's Scary Memo provides yet more evidence how closely linked are torture and the surveillance of every American.

THE TRUTH MISSING FROM ALEXANDER JOEL'S "TRUTH" ABOUT EO 12333

Over at Salon, I've got a piece responding to Office of Director of National Intelligence Civil Liberties Officer Alexander Joel's column purporting to describe the "truth" about EO 12333.

Click through to see this part of my argument:

- Joel resorts to the tired old "target" jargon
- Joel points to PPD 28, which rather than supporting his point, actually shows how broadly the NSA uses bulk collection and therefore how meaningless that "target" jargon is
- Joel doesn't address one of John Napier Tye's points – that current technology allows the NSA to collect US person data overseas
- We know they're doing that in the SPCMA – the Internet

dragnet authority conducted on Internet data collected overseas

But it's Joel's claim about oversight I find most problematic.

Oversight is extensive and multi-layered. Executive branch oversight is provided internally at the NSA and by both the Department of Defense and the Office of the DNI by agency inspectors general, general counsels, compliance officers and privacy officers (including my office and the NSA's new Civil Liberties and Privacy Office). The Department of Justice also provides oversight, as do the Privacy and Civil Liberties Oversight Board and the president's Intelligence Oversight Board. In addition, Congress has the power to oversee, authorize and fund these activities.

As I note in my piece, really what we have is single branch oversight. And that's not going to prevent abusive spying.

Joel's claim, "Oversight [of EO 12333 collection] is extensive and multi-layered," rings hollow. He lists 4 oversight positions at 3 Executive branch agencies, then points to 3 more Executive branch agencies he claims have a role. Having the Executive oversee the Executive spying on Americans poses precisely the kind of threat to our democracy Tye raised.

Then Joel claims, "Congress has the power to oversee, authorize and fund these activities." Of course, that's different from Congress actually using that power. Moreover, the record suggests Congress may not currently have the power to do anything but defund such

spying, assuming they even know about it. Senate Intelligence Committee Chair Dianne Feinstein **admitted** last August that her committee doesn't receive adequate information on EO 12333 collection. Joel's boss, James Clapper, **refused to answer** a question from Senator Amy Klobuchar on EO 12333 violations in a hearing in October. And when Senator Mark Udall **suggested** a "vast trove" of Americans' communications collected overseas should be provided the protections laid out in FISA, Assistant Attorney General John Carlin explained the National Security Division – the part of DOJ he oversees, which has a central role in oversight under FISA – would not have a role in that case because the collection occurred under EO 12333.

In his column, Joel makes no mention of the third branch of government: the Courts. That's because, as ACLU's Patrick Toomey laid out last week, the government **doesn't give** defendants any notice if their prosecutions arise from data collected under EO 12333. Criminal prosecutions are where some of the most important oversight on Executive branch spying takes place. By exempting EO 12333 from any such notice, then, the government is bypassing another critical check on potentially abusive spying.

Back in 1978, our government decided that both Congress and the courts should have a role when the Executive branch spied on Americans. That was the entire premise behind the FISA law. But by moving more and more of its spying overseas, the government can and – apparently, at least to a limited extent – *is* bypassing the oversight accorded through three branches of government.

FISA was written in 1978, before it became so

easy to spy on Americans' domestic communications overseas. FISA Amendments Act partly addressed the new technological reality – by giving the Executive permission to spy on foreigners domestically. But it provided inadequate protections – Sections 703-5 – in return. Those measures, requiring a Court order for targeting Americans who are themselves overseas (but not for targeting Americans' data that transits overseas), simply don't do enough to prevent the government from using this new technological reality from spying on Americans.