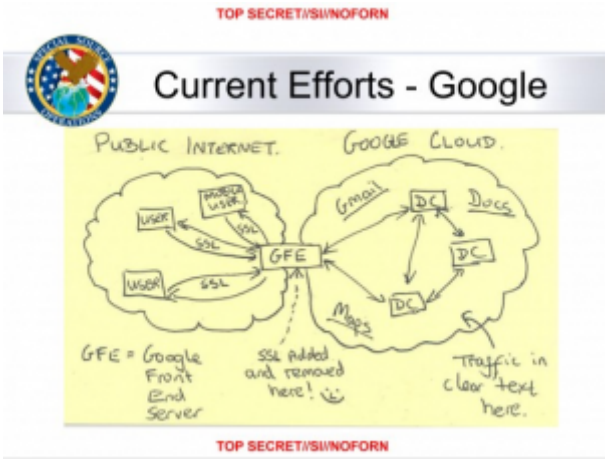
NSA RETURNS TO STEALING FROM YAHOO AND GOOGLE



The entire point of the Protect America Act and FISA Amendments Act was to provide a way for NSA to collect data from Yahoo and Google without stealing it from telecom switches, which is what they had been doing for 6 years. That was the primary goal: provide a legal means, with oversight, to collect intelligence from the multinational US-based Internet companies that dominated the free email market.

Yet, as I've been predicting for weeks, that wasn't good enough for NSA. In addition to all the intelligence they collect legally using PRISM under Section 702 authority, it turns out they've been busy returning to their thieving ways.

> The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.
>
> By tapping those links, the agency has positioned itself to collect at will from among hundreds of millions of user accounts, many of them belonging to

> Americans. The NSA does not keep everything it collects, but it keeps a lot.
>
> According to a top secret accounting dated Jan. 9, 2013, NSA's acquisitions directorate sends millions of records every day from Yahoo and Google internal networks to data warehouses at the agency's Fort Meade headquarters. In the preceding 30 days, the report said, field collectors had processed and sent back 181,280,466 new records – ranging from "metadata," which would indicate who sent or received e-mails and when, to content such as text, audio and video.
>
> The NSA's principal tool to exploit the data links is a project called MUSCULAR, operated jointly with the agency's British counterpart, GCHQ. From undisclosed interception points, the NSA and GCHQ are copying entire data flows across fiber-optic cables that carry information between the data centers of the Silicon Valley giants.

Mind you, the apologists will say that breaking into Yahoo and Google's internal clouds to steal this information isn't stealing because it takes place overseas, and therefore doesn't have to abide by FISA, and therefore just amounts to normal old spying.

Case in point:

> Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight. NSA documents about the effort refer directly to "full take," "bulk access" and "high volume" operations on Yahoo and Google networks. Such large-scale collection of Internet content would be illegal in the United States, but the operations take place overseas, where

> the NSA is allowed to presume that anyone using a foreign data link is a foreigner.
>
> Outside U.S. territory, statutory restrictions on surveillance seldom apply and the Foreign Intelligence Surveillance Court has no jurisdiction. Senate Intelligence Committee Chairwoman Dianne Feinstein has acknowledged that Congress conducts little oversight of intelligence-gathering under the presidential authority of Executive Order 12333 , which defines the basic powers and responsibilities of the intelligence agencies.
>
> John Schindler, a former NSA chief analyst and frequent defender who teaches at the Naval War College, said it was obvious why the agency would prefer to avoid restrictions where it can.
>
> "Look, NSA has platoons of lawyers and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole," he said. "It's fair to say the rules are less restrictive under Executive Order 12333 than they are under FISA."

But as I noted in this post, there's at least an argument to be made that the 2011 John Bates decision ruling Section 702 upstream collection intentional and the existing FAA (that is, far more stringent than the 12333) minimization procedures insufficient under the Fourth Amendment would apply here, making the exposure of US person data under this collection a constitutional violation. And all that's assuming there's a purpose, like terrorism, that would warrant (heh) a special needs exception. With such bulk collection and nonexistent oversight, it's not clear such a case could be made.

So stealing. And in the process doing enormous damage to two important American companies.

There's one odd thing about this article though. Notice the absence of any discussion of Microsoft?

CIVIL LIBERTARIANS TO DIANNE FEINSTEIN: WE TOLD YOU SO

The moment when Dianne Feinstein **should** have called for a comprehensive review of NSA's programs was no later than August 18, when she admitted the Senate Intelligence Committee doesn't get briefed on violations that occur under Executive Order 12333, even though they constitute the bulk of violations.

> The committee does not receive the same number of official reports on other NSA surveillance activities directed abroad that are conducted pursuant to legal authorities outside of FISA (specifically Executive Order 12333), but I intend to add to the committee's focus on those activities.
>
> The committee has been notified—and has held briefings and hearings—in cases where there have been significant FISA compliance issues. In all such cases, the incidents have been addressed by ending or adapting the activity.
>
> [snip]
>
> I believe, however, that the committee can and should do more to independently verify that NSA's operations are appropriate, and its reports of compliance incidents are accurate. This

> should include more routine trips to NSA by committee staff and committee hearings at which all compliance issues can be fully discussed.

While at the time she bought the NSA's roamer myth, it was already clear the NSA was spying on US persons via its bulk collection "overseas," including via some of the more troubling violations. She should have further gotten concerned when both Keith Alexander and James Clapper dodged questions about upstream violations. But then, she was too busy reading factually inaccurate statements about the same collections.

Back in the day, though, making sure the NSA wasn't using Article II to evade oversight used to be one of her chief concerns.

Nevertheless, it took the disclosures of spying on Angela Merkel — and, no doubt, the embarrassment of her party's President, and perhaps growing support for a real investigation — to really rile her up.

> It is abundantly clear that **a total review of all intelligence programs is necessary so that members of the Senate Intelligence Committee are fully informed as to what is actually being carried out by the intelligence community**.
>
> Unlike NSA's collection of phone records under a court order, it is clear to me that certain surveillance activities have been in effect for more than a decade and that the Senate Intelligence Committee was not satisfactorily informed. Therefore **our oversight needs to be strengthened and increased**.
>
> With respect to NSA collection of intelligence on leaders of U.S. allies—including France, Spain, Mexico and Germany—let me state unequivocally: I am totally opposed.

> Unless the United States is engaged in hostilities against a country or there is an emergency need for this type of surveillance, I do not believe the United States should be collecting phone calls or emails of friendly presidents and prime ministers. The president should be required to approve any collection of this sort.
>
> It is my understanding that President Obama was not aware Chancellor Merkel's communications were being collected since 2002. That is a big problem.
>
> The White House has informed me that collection on our allies will not continue, which I support. But **as far as I'm concerned, Congress needs to know exactly what our intelligence community is doing. To that end, the committee will initiate a major review into all intelligence collection programs**. [my emphasis]

I welcome this review — by all accounts the torture review conducted under her supervision is more thorough than anything else we've seen.

But … ah, the torture review.

There's one other reason DiFi should have been quicker to respond to questions Edward Snowden — whom she called a traitor — raised.

In December she finished a 6,000 page report, one key finding of which was that the CIA lied to her community.

Why did she think NSA would be any different?

THE OVERSIGHT BLACK HOLE OF THE MERKEL TAP

In one of the better pieces on White House and anonymous NSA official claims about whether President Obama knew of the wiretaps on Angela Merkel, the NSA spokesperson gets to the crux of the issue.

> "NSA is not a free agent," said NSA spokesperson Vanee Vines. "The agency's activities stem from the National Intelligence Priorities Framework, which guides prioritization for the operation, planning, and programming of U.S. intelligence analysis and collection." The framework is approved by the top leaders of the government, but it leaves the question of how best to gather intelligence to the individual agencies.

This statement gets at why the anonymous NSA source claims that someone — whether it be Keith Alexander or another briefer — informed Obama of the tap on Merkel in 2010 and that he authorized it continue and the White House's rebuttal that he didn't know about the wiretaps on world leaders.

> The account suggests President Barack Obama went nearly five years without knowing his own spies were bugging the phones of world leaders. Officials said the NSA has so many eavesdropping operations under way that it wouldn't have been practical to brief him on all of them.
>
> They added that the president was briefed on and approved of broader intelligence-collection "priorities," but that those below him make decisions about specific intelligence targets.

> The senior U.S. official said that the current practice has been for these types of surveillance decisions to be made at the agency level. “These decisions are made at NSA,” the official said. “The president doesn’t sign off on this stuff.” That protocol now is under review, the official added.

That is, the President approves the National Intelligence Priorities Framework and gets the results of the collection authorized by it, but he may not know specifically how each piece of intelligence was collected. I have no doubt Obama approved a continued focus on EU leaders in the aftermath of the financial crisis, but find it plausible that he did not know that would include monitoring Merkel’s private cell phone.

Here’s how the NIPF describes it working.

> 1. The National Intelligence Priorities Framework (NIPF) is the DNI’s sole mechanism for establishing national intelligence priorities.
> 2. Intelligence topics reviewed by the National Security Council (NSC) Principals Committee (PC) and approved by the President semi-annually shall form the basis of the NIPF and the detailed priorities established by the DNI.
> 3. The NIPF consists of:

> a. Intelligence topics approved by the President.
> b. A process for assigning priorities to countries and non-state actors relevant to the approved intelligence topics.
> c. A matrix showing these priorities.

> 4. The NIPF matrix reflects customers’ priorities for intelligence support and ensures that long-term intelligence

> issues are addressed.
> 5. The NIPF matrix is updated semi-annually, and ad hoc adjustments may be made to reflect changes in world events and policy priorities.
> 6. The ODNI and IC elements shall use the NIPF in allocating collection and analytic resources.

And while I don't doubt that Keith Alexander has had specific conversations with the President about sources and methods, with one exception, the formal process (and therefore the thing bureaucrats will point to in case of embarrassment) works through the NSC.

The exception is this:

> 10. The Assistant Deputy Director of National Intelligence for the President's Daily Brief shall assist the DDNI/A in developing national intelligence priorities during the semi-annual reviews.

That is, the guy in charge of producing and delivering the President's Daily Brief may provide input into this process outside the NSC chain (remember this policy was written under the Bush Administration, which has a rather storied history of demanding intelligence via the daily briefers, probably to hide having obtained it via another source).

The problem with all this, of course, is that it is treated as clandestine intelligence gathering, just like recruiting Human Sources. While it is secret, it is not the kind of covert op that requires deniability and therefore specific Congressional approval.

Indeed, while normally the discovery of a single tap (remember the bug allegedly found in Ecuador's Embassy) will cause a minor diplomatic tiff, the sheer scale of this — and that world leaders are collectively positioned to take advantage of Obama's embarrassment over it —

makes it a bigger deal requiring these non-denial denials.

The bigger problem with this is that it means this massive program (both the bulk collection and the taps on phones) receives very little oversight outside of the Agency and ODNI. The Intelligence Community would — and presumably did — get kudos for all the nifty insights onto how Merkel's political relationships worked (this is her political, not official, phone), but very few questions about what kind of specific operations are happening.

Here's the thing. Unlike many of the domestic and quasi-domestic programs, this probably really is perfectly legal (at least under domestic law — it is being challenged both for violating German and international law). Congress has long left the President's ability to collect foreign intelligence relatively unchecked and we don't extend Constitutional protections to foreigners not in the US.

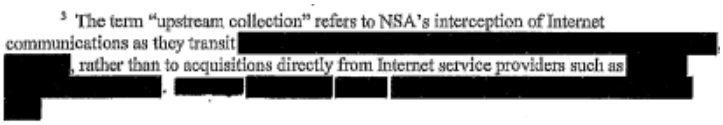
But the other problem with it is that these EO 12333 by technical necessity also collect on US persons. And that may well be illegal. Though if no one outside the Agency and DNI is reviewing, how will we stop it?

The White House keeps inching closer to admitting that there need to be real constraints on what we're doing.

In conjunction with or British partners, we have developed the ability to collect and scan and store much of the telecom traffic in the world. It's a monstrous machine that developed under a reasonable albeit thoroughly outmoded legal structure.

And yet no one noticed that it had turned into a monster.

JAMES CLAPPER VERSUS DOJ (AND NSA) ON UPSTREAM COLLECTION TRANSPARENCY


[redacted] The term "upstream collection" refers to NSA's interception of Internet communications as they transit [redacted], rather than to acquisitions directly from Internet service providers such as [redacted].

Last week, David Ignatius wrote a column declaring the Director of National Intelligence position under James Clapper "Mission Accomplished!" It's mostly a beat sweetener, but I'm intrigued by his claim that James Clapper forced the NSA to declassify more of the 2011 John Bates decision than they wanted to.

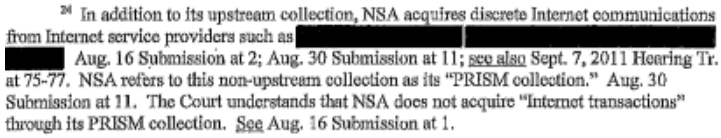
> But there are welcome signs that this jury-rigged structure may finally be starting to work as the DNI responds to budget pressures and the scandals surrounding National Security Agency's surveillance programs. Clapper has recently taken steps that forced the National Security Agency (NSA) to accept greater transparency and stopped the military agencies from wasteful spending on duplicative satellite imagery.
>
> [snip]
>
> One example is Clapper's pressure on the NSA to disclose more about its surveillance programs. The NSA initially wanted to "redact" (a fancy word for censor) far more of a 2011 ruling by the Foreign Intelligence Surveillance Court that the agency had engaged in illegally broad surveillance. Clapper thought NSA lawyers were suppressing too much, so he instructed his general counsel, Robert Litt, to go back through the document and make public more information.

> Clapper ignored NSA and Justice Department protests, including to the White House, and backed Litt's less-redacted version.

That 2011 opinion is one of the most important disclosures so far (and the more I think about it the more I'm convinced it was a dangerous rubber stamp). So I'm grateful as much of it was released as it was.

But I'm intrigued by what this account says of upstream collection (and the searching on US person data collected under FISA Amendments Act) generally.

As the screen cap above shows, even while the opinion made it clear what "upstream" collection is (and other documents released, Dianne Feinstein's public comments, and the footnote below have made it clear the telecoms conduct the collection), it kept the actual language describing the process redacted.



[24] In addition to its upstream collection, NSA acquires discrete Internet communications from Internet service providers such as [redacted] Aug. 16 Submission at 2; Aug. 30 Submission at 11; see also Sept. 7, 2011 Hearing Tr. at 75-77. NSA refers to this non-upstream collection as its "PRISM collection." Aug. 30 Submission at 11. The Court understands that NSA does not acquire "Internet transactions" through its PRISM collection. See Aug. 16 Submission at 1.

Assuming Ignatius description that Clapper pushed for this level of disclosure is correct, consider Clapper's gimmicky efforts to deny or refuse to discuss other upstream collection under EO 12333. That would say Clapper pushed to make more of this FAA upstream collection public, but has gone to some effort to deny the other direct collection under EO 12333.

Meanwhile, remember the way David Kris' paper, which was reviewed by DOJ, managed to raise Internet metadata and EO 12333, but largely indirectly.

They're awfully squirrely about the upstream collection, perhaps because they are increasingly targeting US persons using EO

12333. But it’s worth following.

“TOO MUCH TRANSPARENCY DEFEATS THE VERY PURPOSE OF DEMOCRACY”

In truly bizarre testimony he will deliver to the House Intelligence Committee next week, Paul Rosenzweig argues that “too much transparency defeats the very purpose of democracy.” He does so, however, in a piece arguing that the government needs what amounts to be almost full transparency on all its citizens.

The first section of Rosenzweig analysis talks about the power of big data. It doesn’t provide any actual evidence that big data works, mind you. On the contrary, he points to one failure of big data.

> When we speak of the new form of “dataveillance,” we are not speaking of the comparatively simple matching algorithms that cross check when a person’s name is submitted for review¾when, for example, they apply for a job. **Even that exercise is a challenge for any government, as the failure to list Abdulmutallab in advance of the 2009 Christmas bombing attempt demonstrates.**[11] The process contains uncertainties of data accuracy and fidelity, analysis and registration, transmission and propagation, and review, correction, and revision. Yet, even with those complexities, the process uses relatively simple

> technologically—the implementation is what poses a challenge.
>
> By contrast, other systems of data analysis are far more technologically sophisticated. They are, in the end, an attempt to sift through large quantities of personal information to identify subjects when their identities are not already known. In the commercial context, these individuals are called "potential customers." In the cyber conflict context, they might be called "Anonymous" or "Russian patriotic hackers." In the terrorism context, they are often called "clean skins" because there is no known derogatory information connected to their names or identities. In this latter context, the individuals are dangerous because nothing is known of their predilections. For precisely this reason, this form of data analysis is sometimes called "knowledge discovery," as the intention is to discover something previously unknown about an individual. [my emphasis]

Nevertheless, having not provided evidence big data works, he concludes that "There can be little doubt that data analysis of this sort can prove to be of great value."

The reference to Abdulmutallab is curious. At the beginning of his testimony he repeats the reference.

> In considering this new capability we can't have it both ways. We can't with one breath condemn government access to vast quantities of data about individuals, as a return of "Big Brother"[4] and at the same time criticize the government for its failure to "connect the dots" (as we did, for example, during the Christmas 2009 bomb plot attempted by Umar Farouk Abdulmutallab.

This formulation — and the example of Abdulmutallab even more so — is utterly crazy. **Having** big data is not the same thing as **analyzing** it correctly. Criticism that the Intelligence Community failed to connect the dots — with the UndieBomb attack, but even with 9/11 — assumes **they had the dots** but failed to analyze them or act on that analysis (as the IC did fail, in both cases). Indeed, having big data may actually be an impediment to analyzing it, because it drowns you. And while Rosenzweig suggests the only big data failure with Abdulmutallab involved not placing him on a watch list, that's false. The NSA had wiretaps on Anwar al-Awlaki which, according to the government, collected information tying Abdulmutallab to an attack.

Yet they didn't respond to it.

And you know what? We measly citizens don't know why they didn't respond to it — though we do know that the FBI agents who were analyzing the Awlaki data were … you guessed it! Overwhelmed.

Before anyone involved in government claims that big data helps — rather than hinders — they should have to explain why a full-time tap on Anwar al-Awlaki didn't find the guy who was texting him about a terrorist attack. Particularly in the absence of any other compelling evidence big data works (and the Administration's claims of 54 "terrorist events stopped" barely makes a claim to justify Section 702 collection and certainly doesn't justify Section 215), then logical conclusion is that it in fact does the opposite.

Having made the unsubstantiated claim that giving the government full transparency on citizens and others provides a benefit, Rosenzweig then dismisses any privacy concerns by redefining it.

Part of that involves claiming — reports of the collection of address books notwithstanding — that so long as we don't get identified it doesn't matter.

> The anonymity that one has in respect of these transactions is not terribly different from “real-world anonymity.” Consider, as an example, the act of driving a car. It is done in public, but one is generally not subject to routine identification and scrutiny.

He then proposes we not limit what can be seen, but instead ensure that nothing unjustified can happen to you based on the discovery of something about you.

> In other words, the veil of anonymity previously protected by our “practical obscurity” that is now so readily pierced by technology must be protected by rules that limit when the piercing may happen as a means of protecting privacy and preventing governmental abuse. To put it more precisely, the key to this conception of privacy is that privacy’s principal virtue is a limitation on consequence. If there are no unjustified consequences (i.e., consequences that are the product of abuse or error or the application of an unwise policy) then, under this vision, there is no effect on a cognizable liberty/privacy interest. In other words, if nobody is there to hear the tree, or identify the actor, it really does not make a sound.

If nothing bad in real life happens to you because of this transparency the government should have on citizens, Rosenzweig argues, nothing has happened.

For the moment, I’ll just bracket the many examples where stuff happens in secret — being put on a no fly list, having your neighbor recruited as an informant using data the NSA found, having your computer invaded based on equations of Anonymous with hacker — that still have effects. On those, no one can now assess

whether something bad has happened unjustly, because no one will ever see it. And I'll bracket all the things everyone has ever written about how living in a Panopticon changes behavior and with it community.

Here's how Rosenzweig justifies setting up a (what he fancies to be anonymous but isn't, really) Panopticon while denying citizens the same right to see; here's how he supports his "too much transparency" comment.

> Finally, let me close this statement of principles by noting that none of this is to diminish the significance of the transparency and oversight, generally. Transparency is a fundamental and vital aspect of democracy. Those who advance transparency concerns often, rightly, have recourse to the wisdom of James Madison, who observed that democracy without information is "but prologue to a farce or a tragedy."[13]
>
> Yet Madison understood that transparency was not a supreme value that trumped all other concerns. He also participated in the U.S. Constitutional Convention of 1787, the secrecy of whose proceedings was the key to its success. While governments may hide behind closed doors, U.S. democracy was also born behind them. It is not enough, then, to reflexively call for more transparency in all circumstances. The right amount is debatable, even for those, like Madison, who understand its utility.
>
> What we need is to develop an heuristic for assessing the proper balance between opacity and transparency. To do so we must ask, why do we seek transparency in the first instance? Not for its own sake. Without need, transparency is little more than voyeurism. Rather, its ground is oversight—it enables us to limit and review the exercise of authority.

Man, that series of sentences … "without need, transparency is little more than voyeurism" … "why do we seek transparency for its own sake" are pretty ironic in testimony defending the NSA's collection of records of every phone-based relationship in the US, of having access to 75% of the Internet traffic in the US, and of tapping 35 world leaders just because it could.

But first, Madison.

Because Madison participated in a series of secret meetings the results of which and eventually the details of which were subsequently made public to the entire world, Rosenzweig suggests Madison might support a system where citizens never got to learn how close to all their data the government collects and how it uses it.

Then he argues the only purpose of transparency — the thing separating it from voyeurism — is "oversight," which he describes as limit[ing] and review[ing] the exercise of authority.

If he thought this through, he might realize that even if that's the only legitimate purpose for transparency, it'd still require some oversight over the Executive **and the Legislature** that, in his delegated model of oversight simply would not and could not (and does not) exist. One thing we're learning about the dragnet, for example, is that a good deal of collection on US persons goes on under Executive Order 12333 that gets almost no Congressional review at all. And that's just the most concrete way we're learning how inadequate the oversight practiced by the Intelligence Committees is.

But that's not the only purpose of transparency.

One other purpose of transparency — arguably, the purpose of democracy — is to exercise some rationality to assess the best policies. The idea is that if you debate policies and only then decide on them, you end up with more effective policies overall. It doesn't always work out that way, but the idea, in any case, is that policies subjected to debate end up being

smarter than policies thought up in secret.

It's about having the most effective government.

So in addition to making sure no one breaks the law (Rosenzweig seems unconcerned that NSA has been caught breaking the law and violating court orders repeatedly), transparency — democracy — is supposed to raise the chances of us following better policies.

I presume Rosenzweig figures the debate that goes on within the NSA and within the National Security Counsel adequate to the task of picking the best policies (and the Constitution certainly envisions the Executive having a great deal of that debate take place internally, though surely not on programs as monumental as this).

But here's the thing: the public evidence — whether it be missing the Abdulmutallab texts on an attack, the thin claims of 54 terrorist events, or Keith Alexander's reports that the US has been plundered like a colony via cyberattacks under his watch — it's actually not clear this approach is all that effective. In fact, there's at least reason to believe some parts of the approach in place are ineffective.

That's why we need more transparency. Not to be voyeurs on a bunch of analysts at NSA (really?). But to see if there's a better way to do this.

Ultimately, though, Rosenzweig defeats himself. He's right that we need to find "the proper balance between opacity and transparency" (though he might step back and reconsider what the "very purpose of democracy" is before he chooses that balance). But it is utterly illogical to suggest the balance be set for almost complete transparency when the government looks at citizens — records of all their phone-based relationships and access to 75% of the Internet data — but then argue that delegated transparency (but with almost no transparency on the delegated part) is adequate for citizens looking back at their government.

Related: Homeland Security Czar Lisa Monaco endorses the idea that just because we can collect it doesn't mean we should. Michael Hayden learns surveillance isn't actually all that fun. And Keith Alexander says we should get rid of journalism.

JAMES "TOO CUTE BY HALF" CLAPPER'S DENIAL

James Clapper made a somewhat unprecedented denial of Le Monde's report (French, English) about the NSA's dragnet, denying the eye-popping numbers on the volume of French spying (70.3 million in a month) we do.

> **October 22, 2013**
>
> Recent articles published in the French newspaper Le Monde contain inaccurate and misleading information regarding U.S. foreign intelligence activities. The allegation that the National Security Agency collected more than 70 million "recordings of French citizens' telephone data" is false.
>
> While we are not going to discuss the details of our activities, we have repeatedly made it clear that the United States gathers intelligence of the type gathered by all nations. The U.S. collects intelligence to protect the nation, its interests, and its allies from, among other things, threats such as terrorism and the proliferation of weapons of mass destruction.
>
> The United States values our longstanding friendship and alliance with France and we will continue to

> cooperate on security and intelligence matters going forward.

Now, for what it's worth, this seems the product of somewhat bad translation of the English for the Le Monde article, which started as this,

> Parmi les milliers de documents soustraits à la NSA par son ex-employé figure un graphique qui décrit l'ampleur des surveillances téléphoniques réalisées en France. On constate que sur une période de trente jours, du 10 décembre 2012 au 8 janvier 2013, 70,3 millions d'enregistrements de données téléphoniques des Français ont été effectués par la NSA.

And then a worse translation back into English, which produced this,

> Amongst the thousands of documents extracted from the NSA by its ex-employee there is a graph which describes the extent of telephone monitoring and tapping (DNR – Dial Number Recognition) carried out in France. It can be seen that over a period of thirty days – from 10 December 2012 to 8 January 2013, 70,3 million recordings of French citizens' telephone data were made by the NSA.

I'm not going to explain this perfectly, but effectively it took a verbal that could mean the tape recording or the data notation of calls and turned it into a gerund that has the connotation in English of a discrete tape recording (note also the really cloddish use of the passive in a situation where you wouldn't use it in English).

And from that, Clapper pounced on the "recordings" and presented them – in a quotation taken out of context – as discrete phone calls recorded individually. NSA's not doing that, he says.

But we knew that. What they're doing is intercepting call data in bulk and then sorting through what they want to keep.

It's worth noting that the comment on the Boundless Informant screen Le Monde gets this from, however, refers to a more accurate calls "interceptées." None of that excuses Le Monde's presentation of it as such, particularly not its weak English translation which Clapper exploited (which isn't, however, the actual language that has given François Hollande an opportunity to pretend to be shocked, and his English-only gotcha would be useful in refuting this for actual French readers). But that's one source of the gotcha.

Now, as I said, this is relatively unprecedented. In the recent "interview" with Keith Alexander, NSA issued non-denial denials about info sharing with Israel. But there have been few very specific denials like this one.

And why would there be? Should we now assume all the other facts that have come out, anywhere in the world, are true? That Clapper has gone out of his way to do so, it seems, suggests the IC doesn't dispute any other facts, which is almost certainly not the case, but nevertheless a fair assumption given their attention to this discrete point.

The one exception to this general rule, though, suggests why Clapper may have used this bad translation to claim gotcha! It just so happens to pertain to the WSJ story on upstream Internet collection, which offers this description of how the collection works (note, this would differ from the upstream collection in France in communication type — phone versus Internet — and presumably the degree of filtering going on).

> The systems operate like this: The NSA asks telecom companies to send it various streams of Internet traffic it believes most likely to contain foreign intelligence. This is the first cut of the data.

> These requests don't ask for all Internet traffic. Rather, they focus on certain areas of interest, according to a person familiar with the legal process. "It's still a large amount of data, but not everything in the world," this person says.
>
> The second cut is done by NSA. It briefly copies the traffic and decides which communications to keep based on what it calls "strong selectors"—say, an email address, or a large block of computer addresses that correspond to an organization it is interested in. In making these decisions, the NSA can look at content of communications as well as information about who is sending the data.

The big takeaway from that article was that the initial run on this data at the telecoms have the ability to get 75% of the Internet content in the US, a number just as impressive as the 70.3 million calls in a month.

> The system has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans. In some cases, it retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology, these people say.

To deny that claim, ODNI issued an even more misleading denial (and one that ultimately presented no complaint about the WSJ reporting).

> The reports leave readers with the impression that NSA is sifting through as much as 75% of the United States' online communications, which is simply not true.

That is, as with Le Monde's admittedly misleading bad translations, Clapper denied something other than what the article in chief claimed (though again, I do think Le Monde got legitimately gotchaed here).

Perhaps the most interesting aspect of this is the recurrent efforts to use gimmicks to deny misrepresentations but not the underlying discussion that NSA is getting access to (whether an analyst touches it or not) unbelievable volumes of communications.

In other situations, both Clapper, very aggressively and dishonestly, and Dianne Feinstein, via misinformation, have tried to obscure how much volume NSA accesses with its backbone collection.

It's becoming the one thing they try to deny, over and over, via whatever means no matter how dishonest. And yet thus far, this linguistic gotcha is the closest they've ever come to ever issuing a factually honest denial to the otherwise confirmed fact that they are collecting vast amount of data directly off telecom backbones.

FALSE PROPHET OF ADEQUATE CONGRESSIONAL OVERSIGHT FINDS CONGRESSIONAL IGNORANCE UNNEWSWORTHY

I was going to leave this post, in which Ben Wittes complains that WaPo published details of

NSA's collection of millions of contact lists, which he didn't find at all newsworthy, well enough alone.

> Here the public interest in disclosure seems, at least to me, remarkably weak, after all. At the policy level, the entire story amounts to nothing more than the proposition that NSA is under 12333 collecting large volumes of live-stream data, storing it, and protecting U.S. person material within that data only through minimization requirements. We knew all of that already.
>
> So what does this story reveal that we didn't already know? A specific collection method that people can now frustrate and a particular interest in collecting contact lists. In other words, here the *Post* does not seem to be balancing the costs of the disclosure against its benefit to the public interest. The costs, rather, *are the benefit to the public interest.* Put another way, I can't quite shake the feeling that my old newspaper is now blowing secrets merely for the sake of doing so.

But his response to this post from Conor Freidersdorf convinced me to do a post. He's written about 40 tweets in response, asserting things like, "there is no good argument that this sort of activity is illegal under current law." In all that tweeting, he did not, however, respond to what I thought was a pretty decent argument this sort of activity might be illegal under current law.

Two years ago, then FISA Court Judge John Bates considered the legality of content collected off US switches. He found the practice, as had been conducted for over 3 years, violated both Section 702 of FISA Amendments Act and the Fourth Amendment because it intentionally collected US person data (NSA's apologists

usually obscure this last point, but Bates' opinion was quite clear that this was intentional collection). To make the collection "reasonable" under a special needs exception, he required NSA to follow more stringent minimization procedures than already required under Section 702, effectively labeling some of the data and prohibiting the NSA from using US person data except in limited circumstances.

That collection differs from the contact list collection revealed by the WaPo in several ways:

The contact lists are collected overseas

WaPo's sources are quite clear: this collection would be illegal in the US. They get around that restriction by collecting the data overseas.

> The NSA has not been authorized by Congress or the special intelligence court that oversees foreign surveillance to collect contact lists in bulk, and senior intelligence officials said it would be illegal to do so from facilities in the United States. The agency avoids the restrictions in the Foreign Intelligence Surveillance Act by intercepting contact lists from access points "all over the world," one official said, speaking on the condition of anonymity to discuss the classified program. "None of those are on U.S. territory."

It's not clear whether the contact list counts as metadata or content

The collection reviewed by Bates was clearly content: Internet messages collected because a selector appeared in the body of the message. With the contact lists, I could see the government claiming it was just metadata, and therefore (incorrectly, in my opinion but not in current law) subject to a much lower standard of protection. Except (as noted) WaPo's sources admit this would be illegal if collected in the US, probably because NSA is collecting content

as well.

> Each day, the presentation said, the NSA collects contacts from an estimated 500,000 buddy lists on live-chat services as well as from the inbox displays of Web-based e-mail accounts.
>
> [snip]
>
> Contact lists stored online provide the NSA with far richer sources of data than call records alone. Address books commonly include not only names and e-mail addresses, but also telephone numbers, street addresses, and business and family information. Inbox listings of e-mail accounts stored in the "cloud" sometimes contain content, such as the first few lines of a message.

This data is subjected to a much lower standard of minimization than that imposed by Bates

In his flurry of tweets, Ben keeps repeating that the US person contact lists collected under this program are protected by minimization, so it's all good. But minimization for Executive Order 12333 collection is not as rigorous as minimization under Section 702, and certainly doesn't include the special handling that Bates required to make the Section 702 upstream collection compliant with the Fourth Amendment. So even for those who believe minimization on bulk collection gets you to compliance with the Fourth Amendment, it's unclear whether the minimization provided for **this** collection does, and given Bates' ruling, there's reason to believe it does not.

Neither Congress nor the FISA Court oversee this collection closely

This is the part of the WaPo story that a guy like Ben who wails NAKED! every time someone questions whether there's adequate oversight ought to have noted. A single source claimed this program includes checks and balances. But

as WaPo lays out, these aren't checks and balances like those protecting other US person collections.

> A senior U.S. intelligence official said the privacy of Americans is protected, despite mass collection, because "we have checks and balances built into our tools."
>
> NSA analysts, he said, may not search within the contacts database or distribute information from it unless they can "make the case that something in there is a valid foreign intelligence target in and of itself."
>
> In this program, the **NSA is obliged to make that case only to itself or others in the executive branch**. With few exceptions, intelligence operations overseas fall solely within the president's legal purview. The Foreign Intelligence Surveillance Act, enacted in 1978, imposes restrictions only on electronic surveillance that targets Americans or takes place on U.S. territory.
>
> [snip]
>
> Sen. Dianne Feinstein, the California Democrat who chairs the Senate Intelligence Committee, said in August that **the committee has less information about, and conducts less oversight of, intelligence gathering that relies solely on presidential authority**. She said she planned to ask for more briefings on those programs.
>
> "In general, the committee is far less aware of operations conducted under 12333," said **a senior committee staff member**, referring to Executive Order 12333, which defines the basic powers and responsibilities of the intelligence agencies. **"I believe the NSA would answer questions if we asked them, and**

> **if we knew to ask them, but it would not routinely report these things, and, in general, they would not fall within the focus of the committee.**" [my emphasis]

Here we have DiFi and a senior Senate Intelligence Committee staffer admitting they don't know much about what NSA does under EO 12333. If they know about it, they might ask and might get responses, but otherwise they are largely blind to this collection.

I'm curious. How does Ben claim "we knew of that already" if Senate Intelligence sources are suggesting they didn't? Is Lawfare getting some kind of special briefings that not even SSCI is getting?

If this collection is intentional, it may well be illegal

All of which brings us to the one question on which, I think, the legality of this collection would ride.

Particularly given FISA Amendments Act Section 704, which requires a FISA order to collect content even on Americans overseas (though only in circumstances where those Americans have a reasonable expectation of privacy, which may be how NSA dismisses this requirement), I'm not sure NSA's dodge that this is overseas collection works in this day and age. After all, a judge has now ruled that if the government collects US person content because it fits the terms of its search, it counts as intentional collection (which is why NSA apologists' dishonesty about Bates' ruling on the intentionality of the searches is so important). And NSA appears to be approaching the vast amount of this US person collection using the same strategy they did with domestic upstream collection: admitting they get it, but refusing to quantify it, perhaps out of fear that doing so would undermine claims this was unintentional.

> Although the collection takes place overseas, two senior U.S. intelligence officials acknowledged that it sweeps in the contacts of many Americans. They declined to offer an estimate but did not dispute that **the number is likely to be in the millions or tens of millions**.
>
> [snip]
>
> When information passes through "the overseas collection apparatus," the official added, "the assumption is you're not a U.S. person."
>
> In practice, data from Americans is collected in large volumes — in part because they live and work overseas, but also because data crosses international boundaries even when its American owners stay at home. Large technology companies, including Google and Facebook, maintain data centers around the world to balance loads on their servers and work around outages. [my emphasis]

Ultimately, if the NSA needed new legislation to cover "foreign" data collected transiting US backbone or sitting in US cloud storage, it probably needs new legislation to cover entirely domestic data collected in purportedly "foreign" locales. And it certainly shouldn't use its assumption that this is all foreign as a way out of protections for US person data enshrined by law.

Now all of this is, of course, just my map of why this collection **might not be legal**, even under existing law (but especially noting Bates' 2011 ruling on upstream collection).

But the way we determine whether something is legal or not in this country is in courts. Which brings me back to why it is so curious that Ben ignored the extensive discussion in the WaPo article of one of his favorite topics, the adequacy of oversight.

One reason this is news — one reason it is important and completely justifiable for WaPo to publish this — is it points to an arguably problematic (and even more arguably overreaching) program that **evades almost all oversight**. It can't be deemed legal or not because it simply never gets reviewed in a court (and if it did, the NSA would likely refuse to reveal the extent to which it targeted Americans, like they already did for domestic upstream collection). Indeed, not even Ben's beloved Congressional Oversight Committees (NAKED!) review this.

But I suspect that's by design.

The NSA is knowingly (and admittedly, albeit anonymously) collecting data, probably including content, on millions of Americans by claiming it is foreign collection not subject to domestic laws, Congressional oversight, or the Courts. They may have a nice legal gimmick worked out for themselves that allows them to avoid the implications of Bates' 2011 opinion, but that may be no more than a gimmick.

6 years ago, even Dianne Feinstein expressed concern the government would use EO 12333 to spy on US persons as a way of evading FISA. There's certainly an easy case to make that NSA has done just that. Perhaps that's reason enough to justify publishing this information?

---

6 YEARS LATER, ARE THE INTERNET COMPANIES TRYING TO EXPOSE TELECOMS STEALING

THEIR DATA, AGAIN?

Update: And now this, too, has been halted because of the shutdown (h/t Mike Scarcella). This motion suggests the government asked the Internet companies for a stay on Friday. This one suggests the Internet companies asked the government for access to the classified information in the government filing, but the government told them they can't consider that during the shut-down.

As Time lays out, unlike several of the other NSA-related transparency lawsuits, the fight between the government and some Internet companies (Google, Yahoo, Facebook, Microsoft, and LinkedIn, with Dropbox as amicus) continues even under government shut-down. The government's brief and declaration opposing the Internet bid for more transparency is now available on the FISA Court docket.

Those documents — along with an evolving understanding of how EO 12333 collection works with FISA collection — raise new questions about the reasons behind the government's opposition.

When the Internet companies originally demanded the government permit them to provide somewhat detailed numbers on how much information they provide the government, I thought some companies — Google and Yahoo, I imagined — aimed to show they were much less helpful to the government than others, like Microsoft. But, Microsoft joined in, and it has become instead a showdown with Internet companies together challenging the government.

Meanwhile, the phone companies are asking for no such transparency, though one Verizon Exec explicitly accused the Internet companies of grandstanding.

> In a media briefing in Tokyo, Stratton, the former chief operating officer of Verizon Wireless, said the company is "compelled" to abide by the law in each country that it operates in, and accused

> companies such as Microsoft, Google, and Yahoo of playing up to their customers' indignation at the information contained in the continuing Snowden leak saga.
>
> Stratton said that he appreciated that "consumer-centric IT firms" such as Yahoo, Google, Microsoft needed to "grandstand a bit, and wave their arms and protest loudly so as not to offend the sensibility of their customers."
>
> "This is a more important issue than that which is generated in a press release. This is a matter of national security."
>
> Stratton said the larger issue that failed to be addressed in the actions of the companies is of keeping security and liberty in balance.
>
> "There is another question that needs to be kept in the balance, which is a question of civil liberty and the rights of the individual citizen in the context of that broader set of protections that the government seeks to create in its society."

With that in mind, consider these fascinating details from the government filings.

- The FBI — not the NSA — is named as the classification authority and submits the declaration (from Acting Executive Assistant Director Andrew McCabe) defending the government's secrecy claims
- The government seems concerned about breaking out metadata numbers from content (or non-content from non-content and content, as

Microsoft describes it), even while suggesting this is about providing our "adversaries" hints about how to avoid surveillance
- The government suggests some of what the Internet companies might disclose doesn't fall under FISC's jurisdiction

All of these details lead me to suspect (and this is a wildarsed guess) that what the government is really trying to hide here is how they use upstream metadata collection under 12333 to develop relatively pinpointed requests for content from Internet companies. If the Internet companies disclosed that, it would not only make their response seem much more circumscribed than what we've learned about PRISM, but more importantly, it would reveal how the upstream, unsupervised collection of metadata off telecom switches serves to target this collection.

The FBI as declarant

Begin with the fact that the FBI — and not NSA or ODNI — is the declarant here. I can think of two possible reasons for this.

One, that much of the collection from Internet companies is done via NSL or another statute for which the FBI, not the NSA, would submit the request. There are a number of references to NSLs in the filings that might support this reading. [Correction: FBI is not required to submit NSLs in all cases, but they are in 18 USC 2709, which applies here.]

It's also possible, though, that the Internet companies only turn over information if it involves US persons, and that the government gets all other content under EO 12333. As with NSLs, the FBI submits applications specifically

for US person data, not the NSA. But if that's the case, then this might point to massive parallel construction, hiding that much of the US person data they collect comes without FISC supervision.

And remember — the FBI seems to have had the authority to search incidentally collected (presumably, via whatever means) US person data before the NSA asked for such authority in 2011.

There may be other possibilities, but whatever it is, it seems that the FBI would only be the classification authority appropriate to respond here if they are the primary interlocutor with the Internet companies — at least within the context of collection achieved under the FISA Court's authority.

Breaking out metadata from content numbers and revealing "timing"

While the government makes an argument that revealing provider specific information would help "adversaries" to avoid surveillance, two other issues seem to be of more acute concern.

First, it suggests Google and Microsoft's request to break out requests by FISA provision — and especially Microsoft's request to "disclose separate categories for 'non-content' requests and 'content *and* non-content requests" — brought negotiations to a head (see 2-3). This suggests we would see a pretty surprising imbalance there — perhaps (if my theory that the FBI goes to Internet companies only for US person data is correct) primarily specific orders (though that would seem to contradict the PRISM slide that suggested it operated under Section 702). It also suggests that the Internet companies may be providing either primarily content or primarily metadata, not both (as we might expect under PRISM).

The government is also concerned about revealing "the timing of when the Government acquires certain surveillance capabilities." (see brief 19; the brief references McCabe's discussion of timing, but the discussion is entirely

redacted). That's interesting because these are to a large extent (though not exclusively) storage companies. It may suggest the government is only asking for data stored in the Internet companies' servers, not data that is in transit.

The FISC may not have jurisdiction over all this

Then there are hints that the FISC may not have jurisdiction over all the collection involving the Internet companies. That shows up in several ways.

First, in one spot (page 17) the government refers to the subject of its brief as "FISA proceedings and foreign intelligence collection." In other documents, we've seen the government distinguish FISC-governed collection from collection conducted under other authorities — at least EO 12333. Naming both may suggest that part of the jurisdictional issue is that the collection takes place under EO 12333.

There's another interesting reference to the FISC's jurisdiction, where the government says it wants to reveal information on the programs "overseen by this Court."

> Although the Government has attempted to release as much information as possible about the intelligence collection activities overseen by this Court, the public debate about surveillance does not give the companies the First Amendment right to disclose information that the Government has determined must remain classified.

I'm increasingly convinced that the government is trying to do a limited hangout with the Edward Snowden leaks, revealing only the stuff authorized by FISC, while refusing to talk about the collection authorized under other statutes (this likely also serves to hide the role of GCHQ). If this passage suggests — as I think it might — that the Government is only attempting to release that information overseen by the FISC, then it suggests that part of what the

Internet companies would reveal does not fall under FISC.

Then there are the two additional threats the government uses — in addition to gags tied to FISA orders — to ensure the Internet personnel not reveal this information: nondisclosure agreements and the Espionage Act.

I'm not certain whether the government is arguing whether these two issues — even if formulated in conjunction with FISA Orders — are simply outside the mandate of the FISC, or if it is saying that it uses these threats to gag people engaged in intelligence collection not covered by FISA order gags.

> The review and construction of nondisclosure agreements and other prohibitions on disclosure unrelated to FISA or the Courts rules and orders fall far outside the powers that "necessarily result to [this Court] from the nature of [the] institution," and therefore fall outside the Court's inherent jurisdiction.

Whichever it is (it could be both), the government seems intent on staving off FISC-mandated transparency by insisting that such transparency on these issues is outside the jurisdiction of the Court.

There there's this odd detail. Note that McCabe's declaration is not sworn under oath, but is sworn under penalty of perjury under 18 USC 1746 (see the redaction at the very beginning of the declaration) . Is that another way of saying the FISA Court doesn't have jurisdiction over this matter? [Update: One possibility is that this is shut-down related—that DOJ's notaries who validate sworn documents aren't considered essential.]

The PRISM companies and the poisoned upstream fruit

One more thing to remember. Though we don't know

why, the government had to pay the PRISM companies — that is, the same ones suing for more transparency — lots of money to comply with a series of new orders after John Bates imposed new restrictions on the use of upstream data. I've suggested that might be because existing orders were based on poisoned fruit, the illegally collected US person data collected at telecom switches.

That, too, may explain why PRISM company disclosure of the orders they receive would reveal unwanted details about the methods the government uses: there seems to be some relation between this upstream collection and the requests the Internet companies that is particularly sensitive.

As I have repeatedly recalled, back in 2007, these very same Internet companies tried to prevent the telecoms from getting retroactive immunity for their actions under Bush's illegal wiretap program. That may have been because the telecoms were turning over the Internet companies' data to the government.

They appear to be doing so again. And this push for transparency seems to be an effort to expose that fact.

Update: Microsoft's Amended Motion — the one asking to break out orders by statute — raises the initial reports on PRISM, reports on XKeyscore, and on the aftermath of the 2011 upstream problems (which I noted above). It doesn't talk about any story specifically tying Microsoft to Section 215. However, it lists these statutes among those it'd like to break out.

> 1These authorities could include electronic surveillance orders, see 50 U.S.C. §§ 1801-1812; phyasical search orders, see 50 U.S.C. §§ 1821-1829; pen register and trap and trace orders, see 50 U.S.C. §§ 1841-1846; **business records orders, see 50 U.S.C. §§ 1861-1862**; and orders and directives targeting certain

> persons outside the United States, see 50 U.S.C. §§ 1881-1881g. [my emphasis]

If I'm not mistaken, the motion doesn't reference this article, which described how the government accessed Skype and Outlook, which you'd think would be one of the ones MSFT would most want to refute, if it could. But I've also been insisting that they must get Skype info for the phone dragnet, otherwise they couldn't very well claim to have the whole "phone" haystack.

But the mention of Section 215 suggests they may be included in that order.

Also, we keep seeing physical search orders included in a communication arena. I wonder if that's a storage issue.

Update: One more note about the MSFT Amended Motion. It lists where the people involved got their TS security clearances. MSFT's General Counsels is tied to DOD; the lawyers on the brief all are tied to FBI.

One final detail on MSFT. Though the government brief doesn't say this, MSFT is also looking to release the number of accounts affected by various orders, not just the number of targets (which is what the government wants to release). That's a huge difference.

DAVID KRIS OUTLINES THE INTERNET DRAGNET ELEPHANT

Way back on page 64 (of 67) of former Assistant Attorney General for National Security David Kris' paper "On the Bulk Collection of Tangible Things," he invokes the elephant metaphor the President used to promise more NSA disclosures on multiple programs.

> > What I'm going to be pushing the IC to do is rather than have a trunk come out here and leg come out there and a tail come out there, let's just put the whole elephant out there so people know exactly what they're looking at.
>
> In keeping with the President's direction, the Intelligence Community has released many new details **about the bulk telephony metadata** collection program, as described above. In addition, as also noted above, the FISC itself has released significant new information. **The key remaining question is whether there will be additional, authorized releases concerning intelligence activity that has not been subject to prior, unauthorized releases**. [my emphasis]

Kris uses the President's elephant to ask whether they really will disclose their intelligence programs. He mentions just the phone dragnet (even though the Administration, in response to two FOIAs, also released information about their Section 702 upstream collection programs), even as he suggests the Administration might do well to admit to other programs before they are exposed by an Edward Snowden leak.

Which is interesting, because Kris' paper — in spite of his title and in spite of that reference to the phone dragnet — is really about what the government has declassified (the phone dragnet) as well as what the government has left partly hidden (the Internet dragnet and broader phone dragnet).

Kris discusses the PATRIOT-authorized Internet dragnet along with the phone dragnet

Kris, after all, provides the following facts

about the PATRIOT-authorized Internet dragnet, citing the named sources:

- Internet and telephony metadata was collected starting in 2001, until the 2004 hospital disagreement led to the former being moved to Pen Register/Trap & Trace authority in 2004, which was the first bulk order ("purported" NSA IG Report)
- One company — which the "purported" IG report makes clear was an Internet one and is probably Yahoo — did not participate in the illegal wiretap program ("purported" NSA IG Report)
- The Internet metadata collection ended in 2011 (an ODNI spokesperson in a Charlie Savage story)

Kris also points to four different Administration acknowledgements of the Internet metadata program. He refers to the 2009 and 2011 notice letters to Congress (though he focuses on the phone dragnet language in them), and the James Clapper response to Wyden and 25 other Senators. Perhaps most interestingly, Kris notes that government witness(es) have confirmed the program and the use of PR/TT to authorize it…

> At a July 17, 2013 hearing of the House Judiciary Committee, government witnesses confirmed the pen-trap bulk collection.

But unlike just about every other comment in a

hearing cited in his paper, Kris doesn't quote the exchange, which went like this.

> SUZAN DELBENE: The public also now knows that the telephone metadata collection is under Section 215, the Business Records provision of FISA, and that allows for the collection of tangible things. But we've also seen reports of a now-defunct program collecting email metadata. With regard to the email metadata program that is no longer being operated, can you confirm that the authority used to collect that data was also Section 215?
>
> GEN. COLE: It was not. It was the Pen Register Trap and Trace Authority under FISA, which is slightly different, but it amounts to the same kind of thing. It does not involve any content. It is, again, only to and from. It doesn't involve, I believe, information about identity. It's just email addresses. So it's very similar, but not under the same provision.
>
> REP. DELBENE: And could you have used Section 215 to collect that information?
>
> GEN. COLE: It's hard to tell. I'd have to take a look at that.

The transcript from this hearing is up at the I Con the Record site, so it's unclear why Kris didn't quote it. (Though note, I suspect Cole is wrong, and that the Internet dragnet did include identity, because the government used hybrid orders to get just that before PATRIOT reauthorization in 2006 included that in PR/TTs.) Yet it, like the other 3 references, makes it clear that you don't have to rely on "purported" documents the government won't acknowledge to show official confirmation of the PATRIOT-authorized Internet dragnet.

Kris discusses EO 12333 authorized phone and Internet dragnet

Then he goes further in outlining the Internet (and broader phone) dragnet. Citing the "purported" Ken Wainstein letter and the declassified (but still heavily redacted) End-to-End report, Kris suggests there's more than the PATRIOT-authorized Internet metadata the Administration has semi-admitted; there's broader collection on which the government does even more analysis (this is one instance where he makes it clear the government has used 2511(2)(f) to collect this other information, the significance of which I laid out here).

> The government did not, of course, foreclose data mining, contact chaining,54 or other analysis with respect to metadata responsive to queries,55 or of metadata collected **using methods or programs other than the FISC's bulk collection order** under the FISA tangible things provision.56
>
> 54 Contact-chaining involves the use of "computer algorithms. . . [to create] a chain of contacts linking communications and identifying additional telephone numbers, IP addresses, and e-mail addresses of intelligence interest." Memorandum for the Attorney General, from Kenneth L. Wainstein, Assistant Attorney General, November 20, 2007, at 2, available at http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-data-collectionjustice-department [hereinafter Wainstein Contact Chaining Memo]. As with the NSA Draft IG Report, the government has not acknowledged or declassified this memorandum, as it has for certain other unlawfully disclosed documents, and thus it is referred to here only as a document that is, in fact, available the Internet, but without any suggestion that it is or is not what it purports to be, or that any statements within it are accurate. The

215 Bulk Primary Order discusses contact chaining through queries. 215 Bulk Primary Order at 6.

55 See August 2013 FISC Order at 11-13.

56 Alternative methods of collection would include non-bulk FISA orders, **or what prior NSA Directors in the past have referred to as "vacuum cleaner" surveillance outside the ambit of FISA, under Executive Order 12333 and its subordinate procedures, such as DOD 5240-1.R, and perhaps voluntary production if not otherwise prohibited by law**. See NSA End-to-End Review at 15; August 2013 FISC Order at 10 n.10 ("The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders."); cf. 18 U.S.C. § 2511(2)(f) ("Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978"). A purported September 2006 letter from the Acting General Counsel of NSA to the Counsel for Intelligence Policy at DOJ, Attachment B to the Wainstein Contact Chaining Memo, notes that "**NSA acquires this communications metdata . . . under Executive Order 12333. All of the communications metadata that NSA acquires under this authority should**

> **have at least one communicant outside the United States**." For a discussion of "vacuum cleaner" surveillance, see Kris & Wilson, NSIP § 16:5 & nn.14, 31, § 16:12 & nn.16, 18, § 16:17. For a discussion of DOD 5240-1.R, see Kris & Wilson, NSIP §§ 2:7-2:9, Appendix J. The purported Wainstein Contact Chaining Memo discusses such contact chaining with respect to the "large amount of communications metadata," including metadata associated with persons in the United States, contained in NSA's databases. Wainstein Contact Chaining Memo at 3. The 215 Bulk Primary Order states that the FISA "Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata." 215 Bulk Primary Order at 13 n.15.

Through this very contorted set of footnotes, Kris makes it clear that the dragnet is about far more than just PATRIOT-authorized phone and Internet dragnets. He shows us at least hints of the trunk of the elephant of Internet dragnet that the Administration has thus far been unwilling to reveal on its own, even while both the WSJ and NYT have disclosed parts of it.

Indeed, Kris' efforts to discuss this may well be so contorted because (as he notes on the first page of the paper) it has been subject to "an iterative process of prepublication review."

To understand why those contortions are so fascinating, remember Kris' history.

Kris oversaw efforts to clean up the phone and (almost certainly) Internet dragnets

Kris served in a top national security role in Bush's DOJ, but was not read into Cheney's illegal wiretap program (indeed, Kris successfully lobbied Congress for changes to FISA at the same time Cheney chose not to ask

for changes that would have authorized his illegal program). Then, after he left government, he helped DOJ shore up their public case for the illegal program, but afterwords issued a paper critical of one of Bush's central claims, that the AUMF authorized overriding FISA. Remember, though: that paper addressed only the publicly admitted part of the illegal program — the content collection. It didn't address metadata, which is not electronic surveillance, and therefore not subject to the same objections Kris raised.

Under Obama, Kris returned to DOJ. He was confirmed to be AAG of the National Security Division on March 25, 2009, resigned on January 13, 2011, and left on March 4, 2011. Rather than following the career path of his predecessors (several of whom moved to the White House counterterrorism czar position), Kris moved all the way across the country to serve as General Counsel for a patent troll.

Kris' timing in the Obama DOJ meant he took over NSD not long after DOJ started responding in earnest to Reggie Walton's concerns about the phone dragnet program. Kris would almost certainly have overseen DOJ's side of the process of working through the phone dragnet problems (which is why I suggested he'd be intimately familiar with the End-to-End review he cites to talk about the broader phone dragnet). In September 2009, one of his attorneys at NSD alerted the FISC of additional violations the NSA did not reveal of its own accord. Kris would also have overseen cleaning up the second misrepresentation the government made to FISC, which almost certainly pertains to the Internet dragnet. And he would have left not long before DOJ confessed to the third of three misrepresentations to the FISA Court, that pertaining to upstream collection (the first declaration in the FISA Amendments Act reapplication process was April 20, 2011), though he was gone before the tedious process of working through that misrepresentation. And less than a year after he left, the government

stopped the PATRIOT-authorized Internet dragnet.

Which is another way of saying Kris knows this stuff, especially the problems with both the phone and Internet dragnets, and made real efforts to clean up what were actually problems leftover from the illegal program.

Kris' support for these programs is somewhat ambivalent

Which is why those declaring "major victory" about this paper might want to read more closely. Because Kris' support for the dragnets is somewhat ambivalent.

Even in his case citations supporting the dragnets, Kris seems to be making a different argument than the flunkies who wrote the Administration White Paper on the phone dragnet. Whereas the Administration argues for almost unlimited application of "relevance," Kris' readings of some of the same case citations actually support the practice of pre-filtering where possible (though he supports the Administration claims that pre-filtering is not possible for phone records).

> The question, then, was whether the appropriate "category of materials" to be assessed was "the information-storage devices demanded, or . . . the documents contained within them."88 The court held that it was the documents, in part because "the government has acknowledged that a 'key word' search of the information stored on the devices would reveal 'which of the documents are likely to be relevant to the grand jury's investigation,'" but still tried to insist on receiving all of the storage devices in full.89 Judge Mukasey's decision seems to depend in substantial part on the idea that the government had at its disposal a feasible method of pre-filtering the information to be collected—a concession that the government has not made with

> respect to its bulk collection of telephony metadata.

This is, after all, what happens to the 75% of US Internet traffic accessed via telecom pre-filtering, as described by the WSJ and not actually denied by ODNI which, however, doesn't get mentioned in Kris' paper. Kris is making a better case for NSA to get pre-filtered dragnet data than he is for the phone dragnet as it currently exists.

And, as I'm sure a lot of lawyers will point out, even where Kris makes a "case" to support the dragnet, it's rather thin. For example, on both the issues of using Section 215 to collect data for NSA rather than FBI and the ongoing nature of the production, Kris provides almost no statutory support for his argument dismissing these problems. As such, raising them serves more as a roadmap for challenging the program, not a defense of it. In fact, I think these problems identified by Kris actually explain DOJ's request to delay its filing in the ACLU Section 215 FOIA — so it can account for Kris' arguments.

Moreover, at two points in his paper, Kris suggests the original bulk collection decisions may be fairly shoddy. He suggests FISC may have approved it in 2006 not because the legal case was great, but because it was preferable to have the bulk collection under the supervision of the FISC rather than not.

> More broadly, it is important to consider the context in which the FISA Court initially approved the bulk collection. Unverified media reports (discussed above) state that bulk telephony metadata collection was occurring before May 2006; even if that is not the case, perhaps such collection could have occurred at that time based on voluntary cooperation from the telecommunications providers. If so, the practical question before the FISC in

> 2006 was not whether the collection should occur, but whether it should occur under judicial standards and supervision, or unilaterally under the authority of the Executive Branch.

And as part of his (flawed) argument that Congressional reauthorization of these programs makes them legal, Kris suggests the original decision may have been erroneous.

> The briefings and other historical evidence raise the question whether Congress's repeated reauthorization of the tangible things provision effectively incorporates the FISC's interpretation of the law, at least as to the authorized scope of collection, such that **even if it had been erroneous when first issued**, it is now—by definition—correct. [my emphasis]

And all of that is well before Kris' 3 mentions of the government's reliance on 18 U.S.C. § 2511(2)(f). I'm still trying to figure out whether he is exposing this use, or trying to legitimize it. But Kris may well be saying that the government can (and does) move things under 12333 and 2511(2)(f) when they get problematic under FISC oversight (and if he's not, that's a clear implication of his paper).

(Note, I'm finishing this up while watching the Senate Judiciary Committee, and Keith Alexander just admitted to this 12333 metadata program, though he keeps retreating to talking about the FISC-supervised program.)

As inklings of the program have been exposed, it becomes clear that the last four months of Administration damage control have focused on falsely claiming that the only dragnet is the relatively closely-supervised phone dragnet. That's not true (and it's also not true that only counterterrorism targets are investigated under the dragnet).

Kris' paper hints at that. He hints at that elephant — the massive metadata dragnet — the Administration is still hiding under the bed.

It's what we do with the elephant that is particularly pressing.

WORKING THREAD ON FISA ORDER, OPINION

Here.

(2) Prohibition on cell site may be new with this primary order.

(2) The redaction in FN 3 suggests there was at least one change made in program.

(3) Note Court claims it didn't read White Paper. Which means it pretends it doesn't know that briefings for Congress not as advertised.

(4) inclusion of discovery rules may be new, as would oversight function be.

(5) FISC appears to have no understanding of what 3 hops gives the government. It's data mining.

(5) The incidents in FN 8 appear to be new (because the 2009 ones were about collection, not dissemination, save the ones in late 2009).

(8) The precedent on bulk collections was not mentioned in either 2006 or 2008 opinions.

(9) The grouping argument is similar to one the govt made in Moalin.

(10) Govt has not invoked presumption (though it wouldn't need to).

(16) I'm not so surprised that no telephone companies have challenged Section 215 orders. I'm surprised that no company (still!) has challenged a bulk order.

(20) Mention of metadata in first paragraph makes it really likely that the other decision was the Internet metadata.

(20) Note the inclusion of "affiliated persons" at end of page.

(21) Note the reference to the government's Memorandum of Law, submitted in the first phone dragnet docket. The actual order repeats none of this analysis. Truly, it was one shitty opinion.

(22) Note how the opinion relies on both that original memorandum and a new exhibit from the government.

(22) What's wrong with this logic?

> Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.

This was written 4 months after the Boston Marathon attack, in which someone known to have tried to meet with Chechen terrorists bombed in America. But somehow the Tsarnaevs weren't discovered. And that is because … ?

(25) Note the language in the footnote that is redacted in the letter to Congress. "substantially all of the telephone calls handled by the companies."

My comments on the congressional notice are here.

(Order 3) Note the reference to cell site location. That is new since the April opinion.

(Order 6) The language in paragraph C on "queries … to obtain contact chaining information" is slightly different from the

April opinion.

(Order 10) The first two sentences in footnote 10 were redacted in the previous opinion. These other call detail records likely pertain to 12333 collected foreign data, but it’s possible a reference (whether the court realizes it or not) to subscriber ID obtained via NSL.

(Order 11) The date of the automated query approval — November 8, 2012 — was redacted in the earlier order.