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

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

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

> 2.3 Collection of information. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director.

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

> The Privacy and Civil Liberties Oversight Board just sent a letter to Eric Holder and James Clapper requesting that they have all the Intelligence Committee agencies update what are minimization procedures (though the

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

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

RuppRoge aims to require the IC elements to comply.

> (1) REQUIREMENT FOR IMMEDIATE REVIEW.—Each head of an element of the intelligence community that has not obtained the approval of the Attorney

> General for the procedures, in their entirety, required by section 2.3 of Executive Order 12333 (50 U.S.C. 3001 note) within 5 years prior to the data of the enactment of the End Bulk Collection Act of 2014, shall initiate, not later than 180 days after such enactment, a review of the procedures for such element.

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

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

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

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

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

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

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

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

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

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

And given the government's promise to keep reports of metadata analysis, from that point until sometime several years later, it would be obliged to keep all phone dragnet analysis reports involving Americans. That's because — as is made clear from this Memorandum of Understanding issued sometime after March 2,

2009 — the analysts had no way of identifying the source of the data they were analyzing. The MOU makes clear that analysts were performing queries on data including "SIGINT" (EO 12333 collected data), [redacted] — which is almost certainly Stellar Wind, BRFISA, and PR/TT. So to the extent that any metadata report didn't have a clear time delimited way of identifying where the data came from, the NSA could not know whether a query report came from data collected solely pursuant to presidential authorization or FISC order. (The NSA changed this sometime during or before 2011, and now metadata all includes XML tags showing its source; though much of it is redundant and so may have been collected in more than one program, and analysts are coached to re-run queries to produce them under EO 12333 authority, if possible.)

Finally, the real problem for the NSA is that the data "alerted" illegally up until 2009 — including the 3,000 US persons watchlisted without undergoing the legally required First Amendment review — was done so precisely because when NSA merged its the phone dragnet data with the data collected under Presidential authorization — either under Stellar Wind or EO 12333 — it applied the rules applying to the presidentially-authorized data, not the FISC-authorized data. We know that the NSA broke the law up until about 5 years ago. We know the data from that period — the data that is under consideration for being aged off now — broke the law precisely because of the way the NSA mixed EO 12333 and FISC regulations and data.

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

But since the government agreed to preserve the data collected pursuant to presidential

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

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

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

2008'S NEW AND IMPROVED EO 12333: SHARING SIGINT

As part of my ongoing focus on Executive Order 12333, I've been reviewing how the Bush Administration changed the EO when, shortly after the passage of the FISA Amendments Act, on July 30, 2008, they rolled out a new version of the order, with little consultation with Congress. Here's the original version Ronald Reagan issued in 1981, here's the EO making the changes, here's how the new and improved version from 2008 reads with the changes.

While the most significant changes in the EO were — and were billed to be — the elaboration of the increased role for the Director of National Intelligence (who was then revolving door Booz executive Mike McConnell), there are actually several changes that affected NSA.

Perhaps the most striking of those is that, even while the White House claimed "there were very,

very few changes to Part 2 of the order" — the part that provides protections for US persons and imposes prohibitions on activities like assassinations — the EO actually replaced what had been a prohibition on the dissemination of SIGINT pertaining to US persons with permission to disseminate it with Attorney General approval.

The last paragraph of 2.3 — which describes what data on US persons may be collected — reads in the original,

> In addition, agencies within the Intelligence Community may disseminate information, **other than information derived from signals intelligence**, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

The 2008 version requires AG and DNI approval for such dissemination, but it affirmatively permits it.

> In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, **except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General**.

Given that the DNI and AG certified the

minimization procedures used with FAA, their approval for any dissemination under that program would be built in here; they have already approved it! The same is true of the SPCMA — the EO 12333 US person metadata analysis that had been approved by both Attorney General Mukasey and Defense Secretary Robert Gates earlier that year. Also included in FISA-specific dissemination, the FBI had either just been granted, or would be in the following months, permission — in minimization procedures approved by both the DNI and AG — to conduct back door searches on incidentally collected US person data.

In other words, at precisely the time when at least 3 different programs expanded the DNI and AG approved SIGINT collection and analysis of US person data, EO 12333 newly permitted the dissemination of that information.

And a more subtle change goes even further. Section 2.5 of the EO delegates authority to the AG to "approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes." In both the original and the revised EO, that delegation must be done within the scope of FISA (or FISA as amended, in the revision). But in 1981, FISA surveillance had to be "conducted in accordance with that Act [FISA], **as well as this Order**," meaning that the limits on US person collection and dissemination from the EO applied, on top of any limits imposed by FISA. The 2008 EO dropped the last clause, meaning that such surveillance **only** has to comply with FISA, and not with other limits in the EO.

That's significant because there are at least three things built into known FISA minimization procedures — the retention of US person data to protect property as well as life and body, the indefinite retention of encrypted communications, and the broader retention of

"technical data base information" — that does not appear to be permitted under the EO's more general guidelines but, with this provision, **would** be permitted (and, absent Edward Snowden, would also be hidden from public view in minimization procedures no one would ever get to see).

Given that Section 2.5 would thus permit the collection of US person data so long as it was dubbed "technical data base information," consider the way the intelligence mandate for a number of elements of the intelligence community (including DIA, FBI, DOD and its subcomponents generally, Coast Guard, NRO, NGA, and INR, in addition to NSA, but curiously not the CIA) were newly laid out. Each of these elements is permitted to collect intelligence to support national **and departmental** missions. Here's how that language appears as it applies to the NSA:

> Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;
>
> [snip]
>
> Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

Curiously, this change comes with the elimination of the 1981 clause authorizing NSA's "Conduct of research and development to meet the needs of the United States for signals intelligence and communications security" (though there is a similar clause in the 2008 EO applying to both the Intelligence Community as a whole and DOD specifically, which would both apply to NSA). NSA still collects and uses the data it needs to conduct research to advance the SIGINT mission, it appears, but as it seems in

the 2008 EO, it does so in the name of advancing the Department's goals, not the nation's.

In 1981, only DOD had such a departmental mandate. Extending it to these other agencies and departments seems to give them a recursive purpose, the mandate to collect intelligence to serve their own department.

And all this comes in an EO that seems to envision SIGINT playing a bigger role in US intelligence (which makes sense, given that's what we know to have happened). The 1981 EO explicitly calls for a balance between, "technical collection efforts and other means." The 2008 EO eliminates that.

In addition, the 2008 description of both the CIA and FBI's roles limits their focus to human and human-enabled sources (which is particularly curious given that FBI actually has a key role in SIGINT collection).

> (A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;
>
> (B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

At the same time, the revised EO designates the Director of NSA as the functional manager for SIGINT, seemingly both within and outside of the US.

As I said, none of that should be surprising: it reflects both what we knew before last June, and has been reinforced with much of what we've learned with the Snowden leaks. But it does

reflect a codification of that change that I don't think got much notice at the time, even in spite of the EO's revision coming so quickly on the heels of FAA.

There are two more items of interest that affect the potential scope of information sharing, and this applies to both NSA and other elements of the intelligence community (including, to the extent permitted by law, CIA).

First, in one of the changes the Bush Administration hailed at the time, the EO envisions information sharing outside of the Federal government, to state, local, and tribal governments, and to the private sector.

> (f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

This language is repeated several times in the EO.

In a far more subtle change, section 2.6(d) allows intelligence entities to cooperate not just with domestic law enforcement, but also with "other civil authorities" so long as it is not otherwise legally precluded. I can only begin to grasp what the Bush Administration had in mind with this. But at least in the case of NSA, in the face of endless cyber-fearmongering, I can imagine it might support NSA partnering with civil agencies overseeing critical infrastructure (to the extent that that infrastructure is owned by civil authorities and not the private sector).

In 2008, even as the Bush Administration insisted that protections on US person data didn't change with EO 12333's revision, it appears they did change those protections to allow the dissemination of SIGINT on US persons, potentially even to local governments and private entities.

I suspect many, perhaps most, of the changes affecting NSA were not actually new changes. As we know, John Yoo had pixie dusted EO 12333 to hide what the Bush Administration was doing with SIGINT. And at least as late as December 2007, Sheldon Whitehouse believed that pixie dust to remain in effect. So I think it likely that the NSA-related changes simply reflect what Bush had been doing since 2001 in any case.

But in retrospect, the changes to EO 12333 might have raised more alarm about the growing role of the NSA and the dissemination of the data on US persons it collected.

IMPORTANT: CHANGES TO SECTION 215 DRAGNET WILL NOT CHANGE TREATMENT OF EO 12333 METADATA

In their Angry Birds stories, both the Guardian and NYT make what I believe is a significant error. They suggest changes in the handling of the Section 215-collected phone metadata will change the way NSA handles EO 12333-collected phone metadata.

Guardian:

> Data collected from smartphone apps is subject to the same laws and

> minimisation procedures as all other NSA activity — procedures which US president Barack Obama suggested may be subject to reform in a speech 10 days ago. But the president focused largely on the NSA's collection of the metadata from US phone calls and made no mention in his address of the large amounts of data the agency collects from smartphone apps.

NYT:

> President Obama announced new restrictions this month to better protect the privacy of ordinary Americans and foreigners from government surveillance, including limits on how the N.S.A. can view "metadata" of Americans' phone calls — the routing information, time stamps and other data associated with calls. But he did not address the avalanche of information that the intelligence agencies get from leaky apps and other smartphone functions.

Here's what the President actually said, in part, about phone metadata:

> I am therefore ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk meta-data.

That is, Obama was speaking **only** about NSA's treatment of Section 215 metadata, not the data — which includes a great amount of US person data — collected under Executive Order 12333.

To be clear, both Guardian and NYT were distinguishing Obama's promises from the treatment extended to the leaky mobile data app. But they incorrectly suggested that all phone metadata, regardless of how it was collected,

receives the same protections.

Section 215 metadata has different and significantly higher protections than EO 12333 phone metadata because of specific minimization procedures imposed by the FISC (arguably, the program doesn't even meet the minimization procedure requirements mandated by the law). We've seen the implications of that, for example, when the NSA responded to being caught watch-listing 3,000 US persons without extending First Amendment protection not by stopping that tracking, but simply cutting off the watch-list's ability to draw on Section 215 data.

Basically, the way NSA treats data collected under FISC-overseen programs (including both Section 215 and FISA Amendments Act) is to throw the data in with data collected under EO 12333, but add query screens tied to the more strict FISC-regulations governing production under it. This post on federated queries explains how it works in practice. As recently as 2012 at least one analyst improperly searched on US person FAA-collected content because she didn't hit the right filter on her query screen.

> [T]he NSA analyst conducted a federated query using a known United States person identifier, but forgot to filter out Section 702-acquired data while conducting the federated query.

That's it. If the data is accessed via one of the FISC-overseen programs, US persons benefit from the additional subject matter, dissemination, and First Amendment protections of those laws or FISC's implementation of them (and would benefit from the minor changes Obama has promised to both Section 215 and FAA).

But if NSA collected the data via one of its EO 12333 programs, it does not get get those protections. To be clear, it does get some dissemination protection and can only be accessed with a foreign intelligence purpose, but that is much less than what the FISC

programs get. Which leaves the NSA a fair amount of leeway to spy on US persons, so long as it hasn't collected the data to do so under the programs overseen by FISC. And when it collects data under EO 12333, it is a lot easier for the NSA to spy on Americans.

The metadata from leaky mobile apps almost certainly comes from EO 12333 collection, not least given the role of GCHQ and CSEC (Canada's Five Eyes' partner) to the collection. The Facebook and YouTube data GCHQ collects (just reported by Glenn Greenwald working with NBC) surely counts as EO 12333 collection.

NSA's spokeswoman will say over and over that "everyday" or "ordinary" Americans don't have to worry about their favorite software being sucked up by NSA. But to the extent that collection happens under EO 12333, they have relatively little protection.

HOW NSA SPIES ON FIRST AMENDMENT PROTECTED SPEECH: THE EO 12333 LOOPHOLE

As important as the fact that NSA was illegally watch-listing 3,000 US Persons is what they did once they got caught doing so.

They kept watch-listing them.

As I noted, NSA's solution to the problem that it had put 3,000 US Persons on its contact-chaining and alert list without doing the First Amendment review required by Section 215 was simply to move them off the list available for use with Section 215 data.

> NSA remedied this compliance incident by re-designating all such telephone identifiers as non RAS-approved for use as seed identifiers in early February 2009.

The NSA continued its alert list function after the problems with it were discovered; it just restricted its use to data collected under EO 12333. Which appears to mean these 3,000 US persons would continue to have their communications that came up in EO 12333 collections (which would be collected outside of the country) watch-listed. That wouldn't give the NSA as much data about their conversations, granted, but they chose to do that rather than affirm that they weren't watch-listing these people solely because of First Amendment protected activities.

That suggests the NSA could — and may have, in at least some of these cases — spy on Americans' because of their speech or religion or politics, so long as they did so only using collections for which the First Amendment protections do not attach.

Now, we don't know whether and how many of those 3,000 people were targeted for their First Amendment activities. But seeing NSA's behavior here does raise questions about the US person described in this story about the NSA's efforts to discredit ideological foes of the US.

One of 6 "radicalizers" NSA sought discrediting information on in 2012 is a US person (though living overseas). The NSA used contact chaining to measure the targets' (limited, in the case of the English speakers) ties to extremists. And then it collected things like their online porn habits.

But the thing is, it appears that the impetus for this porn-sniffing pertained only to the NSA's very expansive disagreement with the 6 "radicalizers" ideology.

It was about their speech, including the speech

of the US person.

It appears the NSA believes its mandate includes spying on Americans for their protected speech, just so long as it does so using their EO 12333 authorities.

FEDERATED QUERIES AND EO 12333 FISC WORKAROUND

Particularly given the evidence NSA started expanding its dragnet collection overseas as soon as the FISA Court discovered it had been breaking the law for years, I've been focusing closely on the relationship between the FISA Court-authorized dragnets (which NSA calls BR FISA — Business Records FISA — and PR/TT — Pen Register/Trap and Trace — after the authorities used to collect the data) and those authorized under Executive Order 12333.

This document — Module 4 of a training program storyboard that dates to late 2011 — provides some insight of how NSA trained its analysts to use international collections to be able to share data otherwise restricted by FISC.

The module lays out who has access to what data, then describes how analysts look up both the Reasonable Articulable Suspicion (RAS) determinations of identifiers they want to query on, as well as the BR and PR/TT credentials of those they might share query results with. It also describes how "EAR" prevents an analyst from querying BR or PR/TT data with any non-RAS approved identifier. So a chunk of the module shows how software checks should help to ensure the US-collected data is treated according to the controls imposed by FISC.

But the module also describes how a software

interface (almost certainly MARINA, the metadata database) manages all the metadata collected from all over the world.

All of it, in one database.

So if you do what's called a "federated" query with full BR and/or PR/TT credentials — meaning it searches on all collections the analyst has credentials for, with BR and PR/TT being the most restrictive — you may pull metadata collected via a range of different programs. Alternately, you can choose just to search some of the collections.

> When launching analysts with [redacted] the appropriate BR or PR/TT credentials have the option to check a box if they wish to include BR or PR/TT metadata in their queries. If an analyst checks the "FISABR Mode" or "PENREGISTRY Mode" box when logging into [redacted] will perform a federated query. This means that in addition to either BR or PR/TT metadata, [redacted] will also query data collected under additional collection authorities, depending on the analyst's credentials. Therefore, when performing a query of the BR or PR/TT metadata, analysts will potentially receive results from all of the above collection sources. Users of more recent versions of [redacted] do have the option, however, to "unfederate" the query, and pick and choose amongst the collection sources that they would like to query (10)

Back in 2009, when NSA was still working through disclosures of dragnet problems to FISC, analysts apparently had to guess where the data they were querying came from (which of course is an implicit admission that BR data had been improperly treated with weaker EO 12333 protections for years). But by 2011 they had worked it out so queries showed both what SIGAD (collection point) the metadata came from, as

well as (using a classification mark) its highest classification.

> It is possible to determine the collection source or sources of each result within the chain by examining the Producer Designator Digraph (PDDG)/SIGINT Activity Designator (SIGAD) and collection source(s) at the end of the line.
>
> If at least one source of a result is BR or PR/TT metadata, the classification at the beginning of the line will contain the phrases FISABR or PR/TT, respectively. In addition, in the source information at the end of the line, the SIGAD [redacted] BR data can be recognized by SIGADs beginning with [redacted] For PR/TT, data collected after October 2010 is found [redacted] For a comprehensive listing of all the BR and PR/TT SIGADs as well as information on PR/TT data collected prior to November of 2009, contact your organization's management or subject matter expert.
>
> Since it is possible that one communication event will be collected under multiple collection authorities (and multiple collection sources), not all of the results will be unique to one collection authority (or collection source). Keep in mind that the classification at the beginning of each result only indicates the highest level classification of that result, and does not necessarily reflect whether a result was unique to one collection authority (or collection source). If a result was obtained under multiple authorities (or sources), you will see more [redacted] (15-16)

In other words, analysts will be able to see from their results where the results come from.

If a query result includes data only from BR or PR/TT sources, then the analyst can't share the result with anyone not cleared into those programs without jumping some hoops. But if a query result showed other means to come up with the same results from a BR or PR/TT search (that is, if EO 12333 data would return the same result), then the result would not be considered a BR- or PR/TT-unique result, meaning the result could be shared far more widely. (Note, this passage also provides more details about the timing of the Internet metadata shutdown, suggesting it may have lasted from November 2009 to October 2010.)

> Sharing restrictions in the FISC Orders only apply to unique BR or PR/TT query results. If query results are derived from multiple sources and are not unique to BR and PR/TT alone, the rules governing the other collection authority would apply. (17)

After noting this, the training storyboard spends 5 pages describing the restrictions on dissemination or further data analysis of BR and PR/TT results, even summaries of those results.

Then it returns to the point that such restrictions only hold for BR- or PR/TT-unique results and encourages analysts to run queries under EO 12333 so as to be able to get a result that can be shared and further exploited.

> However, as we've discussed, not all BR or PR/TT results are unique. If a query result indicates it was derived from another collection source in addition to BR or PR/TT, the rules governing the other collection authority would apply to the handling an d sharing of that query result. For example, this result came from both BR and E.O. 12333 collection; therefore, because it is not unique to BR information, it would be ok to inform non- BR cleared individuals of the fact of this communication, as well

> as task, query, and report this information according to standard E.O. 12333 guidelines.
>
> In summary, if a query result has multiple collection authorities, analysts should source and/or report the non-BR or PR/TT version of that query result according to the rules governing the other authority. But if it is unique to either the BR or PR/TT authority then it is a unique query result with all of the applicable BR and PR/TT restrictions placed on it. In both cases, however, analysts should not share the actual chain containing BR or PR/TT results with analysts who do not have the credentials to receive or view BR or PR/TT information. In such an instance, if it is necessary to share the chain, analysts should re-run the query in the non-BR or non-PR/TT areas of [redacted] and share that .cml. (22)

Let me be clear: none of this appears to be illegal (except insofar as it involves a recognition it is collecting US person data overseas, which may raise issues under a number of statutes). It's just a kluge designed to use the US-based dragnet programs to pinpoint results, then use EO 12333 results to disseminate widely.

It does, obviously, raise big questions about whether the numbers reported to Congress on dragnet searches reflect the real number of searches and/or results, which will get more pressing if new information sharing laws get passed.

Mostly, though, it shows how NSA uses overseas collection to collect the same data on Americans without the restrictions on sharing it.

There are a lot of likely reasons to explain why the NSA stopped collecting Internet metadata in the US in 2011 (seemingly weeks after this

version of the storyboard, ~~though they would still be able to access the PR/TT metadata for 5 years~~ Update 11/20/14: they destroyed the PRTT data in December 2011). But it is clear the overseas collection serves, in part, to get around FISC restrictions on dissemination and further analysis.

Updated: Added explanation for BR FISA and PR/TT abbreviations.

ARTICLE II IS ARTICLE II: EO 12333 AND PROTECT AMERICA ACT, FISA AMENDMENTS ACT, AND FISC

I'm reading a very old SSCI hearing on FISA today — from May 1, 2007, when then Director of National Intelligence Mike McConnell initiated the push for the Protect America Act.

Given recent revelations that NSA continues to conduct some collection under EO 12333 — including the address books of people all over the world, including Americans — I thought this part of the hearing might amuse some of you.

> SEN. FEINGOLD: I thank the witnesses for testifying today. **Can each of you assure the American people** that there is not — and this relates to what — the subject Senator Wyden was just discussing — **that there is not and will not be any more surveillance in which the FISA process is side-stepped based on arguments that the president has independent authority under Article II** or the authorization of the use of military force?

> MR. McCONNELL: Sir, the president's authority under Article II is – – are in the Constitution. So if the president chose to exercise Article II authority, that would be the president's call. What we're attempting to do here with this legislation is to put the process under appropriate law so that it's conducted appropriately to do two things – protect privacy of Americans on one hand, and conduct foreign surveillance on the other.
>
> SEN. FEINGOLD: My understanding of your answer to Senator Wyden's last question was that there is no such activity going on at this point. In other words, whatever is happening is being done within the context of the FISA statute.
>
> MR. McCONNELL: That's correct.
>
> SEN. FEINGOLD: Are there any plans to do any surveillance independent of the FISA statute relating to this subject?
>
> MR. McCONNELL: None that – none that we are formulating or thinking about currently. But I'd just highlight, **Article II is Article II**, so in a different circumstance, I can't speak for the president what he might decide.
>
> SEN. FEINGOLD: Well, Mr. Director, Article II is Article II, and that's all it is. In the past you have spoken eloquently about the need for openness with the American people about the laws that govern intelligence activity. Just last summer, you spoke about what you saw as the role of the United States stating that, quote, "Because of who we are and where we came from and how we lived by law," unquote, it was necessary to regain, quote, "the moral high ground." Can you understand why the American people might question the value of new statutory authorities when you

> can't reassure them that you consider current law to be binding? And **here, of course, you sound like you're disagreeing with my fundamental assumption, which is that Article II does not allow an independent program outside of the FISA statute, as long as the FISA statute continues to read as it does now that it is the exclusive authority for this kind of activity**.
>
> MR. McCONNELL: Sir, I made those statements because I believe those statements with regard to moral high ground, and so on. I live by them. And what I'm attempting to do today is to explain what it is that is necessary for us to accomplish to be able to conduct the appropriate surveillance to make – to protect the American people, consistent with the law.
>
> SEN. FEINGOLD: Let me ask the other two gentlemen. General Alexander, on this point with regard to Article II, I've been told that there are no plans to take warrantless wiretapping in this context, but I don't feel reassured that that couldn't reemerge.
>
> LTG ALEXANDER: Well, I agree with the way Director McConnell laid it out. I would also point out two things, sir. The program is completely auditable and transparent to you so that you and the others – and Senator Rockefeller, I was remiss in (not) saying to you and Senator Bonn thank you for statements about NSA. They are truly appreciated. Sir, **that program is auditable and transparent to you so that you as the oversight can see what we're doing**. We need that transparency and we are collectively moving forward to ensure you get that. And I think that's the right thing for the country. But we can't change the Constitution. We're

> doing right now everything that Director McConnell said is exactly correct for us to.
>
> SEN. FEINGOLD: Well, here's the problem. **If we're going to pass this statute, whether it's a good idea or a bad idea, it sounds like it won't be the only basis on which the administration thinks it can operate**. So in other words, **if they don't like what we come up with, they can just go back to Article II**. That obviously troubles me. Mr. Wainstein?
>
> MR. WAINSTEIN: Well, Senator, as the other witnesses have pointed out, the Article II authority exists independent of this legislation and independent of the FISA statute. But to answer your question, the surveillance that was conducted, as the attorney general announced, that was conducted pursuant to the president's terrorist surveillance program, is now under FISA Court order.

Here are the documents in which, in an effort starting the previous year and lasting until January 2008, Ken Wainstein pushed to allow contact chaining on Internet metadata collected under both EO 12333 and FISA orders of Americans.

And I just love that Keith Alexander has been repeating that line — "auditable and transparent" — for over 6 years during which his work has been neither.

Update: Dianne Feinstein, who used to care deeply about this issue, asked roughly the same questions.

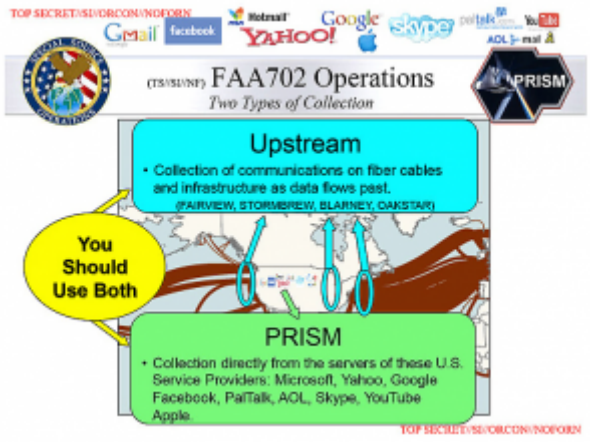
> SEN. DIANNE FEINSTEIN (D-CA): Here's the question: Does the administration still believe that it has the inherent authority to conduct electronic surveillance of the type done under the

> TSP without a warrant?
>
> MR. McCONNELL: Ma’am, the effort to modernize would prevent an operational necessity to do it a different way. So let me – I’m trying to choose my words carefully.
>
> SEN. FEINSTEIN: Yes, but my question is very specific. Does the president still believe he has the inherent authority to wiretap outside of FISA? It’s really a yes or no question.
>
> MR. McCONNELL: No, ma’am, it’s not a yes or no question.
>
> SEN. FEINSTEIN: Oh –
>
> MR. McCONNELL: Sorry – I’m sorry to differ with you. But if you’re asking me if the president is abrogating his Article II responsibilities, the answer is no. What we’re trying to frame is – there was an operational necessary for TSP that existed in a critical period in our history, and he chose to exercise that through his Article II responsibility. We’re now on the other side of that crisis, and we’re attempting to put it consistent with law, so it’s appropriately managed and subjected to the appropriate oversight.
>
> SEN. FEINSTEIN: Well, the way I read the bill, very specifically, the president reserves his authority to operate outside of FISA.

UPSTREAM US PERSON

COLLECTION: EO 12333 AND/OR FISA?

Keith Alexander had a really bizarre response to a question from Mazie Hirono in Tuesday's hearing.



> SEN. HIRONO: I have one more question, Mr. Chairman. General Alexander, is PRISM the only intelligence program NSA runs under FISA Section 702?
>
> GEN. ALEXANDER: Well, PRISM was (the statement ?), but, yes. Essentially, the only program was that – that, you know, is PRISM under 702, which under – operates under that authority for the court. But we also have programs under 703, 704 and 705.

Perhaps he was confused by her question (which came in the context of questions about the NYT's report on the construction of dossiers, potentially on Americans). But he seems to have claimed that PRISM – the collection of Internet content from Internet providers under Section 702 – is the only way the NSA uses FISA Amendments Act to collect content.

Not only does the PRISM slide above belie that (and there's also phone content that is not covered under PRISM).

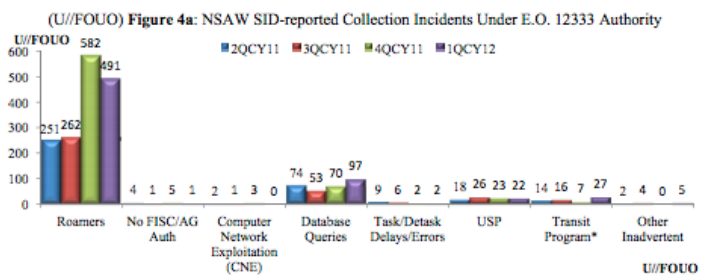
But the government itself released the October 3, 2011 John Bates FISC opinion (and other related documents) which describes the

government's collection of Internet transactions directly from the phone company switches (see footnote 24 where Bates distinguishes between the two kinds of Section 702 Internet collection). In an attempt to spin this collection as a big mistake last week, Dianne Feinstein even confirmed that this "upstream" collection comes from the backbone operated by the phone companies.

> In mid 2011, NSA notified the DOJ, the DNI, and the FISA court, and House and Senate Intelligence Committees, of a series of compliance incidents impacting a subset of NSA collection under Section 702 of FISA, known as upstream collection.
>
> This comprises about 10 percent of all collection that takes place under 702, and occurs when NSA obtains Internet communications, such as e-mails, from certain U.S. companies that operate the Internet background;[sic] i.e., the companies that own and operate the domestic telecommunication lines over which Internet traffic flows.

So there's PRISM, there's phone content collection, and there's the upstream Internet collection from the phone companies' switches. All operated, per the 2011 Bates memo, under Section 702 (and therefore overseen by the FISA Court and Congress).

Which is why I've been pondering this chart and related explanation, from NSA's internal review of compliance incidents for the first quarter of 2012.



The chart shows all the violation incidents NSA discovered under programs authorized under Executive Order 12333 — the EO that covers entirely foreign collection, over which FISC and Congress exercise much less oversight than FISA. And what NSA calls "Transit Program" violations appear in the EO 12333, not the FISA, chart. In the first quarter of 2012 (the first quarter after the government started to resolve the 702 upstream collection problems laid out in the Bates memo), Transit Program violations went up from 7 in a quarter to 27.

NSA describes Transit Program violations this way.

> (TS//SI//REL TO USA, FVEY) International Transit Switch Collection*: International Transit switches, FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251), and SILVERZEPHYR (US-3273), are Special Source Operations (SSO) programs authorized to collect cable transit traffic passing through U.S. gateways with both ends of the communication being foreign. When collection occurs with one or both communicants inside the U.S., this constitutes inadvertent collection. From 4QCY11 to 1QCY12, there was an increase of transit program incidents submitted from 7 to 27, due to the change in our methodology for reporting and counting of these types of incidents,

That is, these "Transit Program" violations reflect the collection of US person data in upstream collection, the very same problem described in the Bates opinion.

As I've been puzzling through why Transit Program violations would appear under EO 12333 rather than FISA, I wondered whether NSA collects off switches under both authorities — some content that the telecoms provide after doing an initial screening (as described in this

WSJ article and backhandedly confirmed by the DNI), and some programs that the NSA collects and sorts off undersea cables itself. Both FAIRVIEW and STORMBREW show up — seemingly as Section 702 collection — on the PRISM slide above, but ORANGEBLOSSOM and SILVERZEPHYR don't (WSJ also lists OAKSTAR and LITHIUM).

If so, though, you'd expect NSA to be finding violations under both authorities, because we know the government collects US person data under the 702 authorized upstream collection (they call this unintentional but Bates deemed it intentional).

This is all the more confusing given the way former Assistant Attorney General David Kris discusses "vacuum cleaner" collection taking place under EO 12333. His paper is on metadata collection, not content, but the vacuum cleaner (that is, dragnet) collection collects content as well (and the distinction may get distorted in discussions of Internet packets).

I don't, yet, know the answer to this question, but the question itself raises several others:

- Given that there's not a 702-authorized Transit Program violation category, does that mean NSA wasn't and may still not be tracking it? That doesn't make sense, because there are greater mandates to track these things under 702.
- If there wasn't a 702-authorized Transit Program violation category before the revelations to John Bates, is it possible NSA instead treated upstream

collection as authorized by 12333 so as not to have to report these violations?

- Are these known violations being reported now? Are they getting reported to Congress and the Court? Or has the NSA simply decided they're not violations since Bates has okayed them, sort of, as intentional collection?
- If some of the upstream collection yielding US person content operates under 12333, does it have to be treated under any minimization rules?
- What do the 7 and 27 violation numbers reflect in relation to the figures of 10,000 SCT and 46,000 MCT estimates involving US persons provided to Bates?
- Did these violations ever get reported to Congress and the FISC?

In short, either all this upstream collection falls under 702, in which case there's a big question why NSA tracks it as 12333 collection. Or the NSA's ability to operate upstream collection under both authorities raises real questions about the protections it accords US person data collected under the 12333 collection.

Update: Two more things on this.

First, remember back in 2001, John Yoo pixie dusted EO 12333, basically holding the President could change the content of it without changing

the language of it publicly. That was done, according to Sheldon Whitehouse, to permit the government to "wiretap Americans traveling abroad." But I suspect it was done to permit the government to "wiretap Americans' communications traveling abroad" — that is, American Internet traffic that transits foreign switches.

That said, I suspect the 2010 OLC memo on using 2511(2)(f) for collection was meant to clean up some of that (and also Yoo's reliance on claiming the Fourth Amendment didn't apply in DOD searches of entire apartment buildings if they were searching for terrorists).

Also, remember that the language of the 2008 Yahoo opinion makes it clear that the Protect America Act — Section 702's predecessor — relied on 12333 for particularity. While we should soon learn more (FISC is releasing much more of this opinion and underlying documents), it seems that PAA was treated as a nested program within 12333.

JAMES CLAPPER PROVES INADEQUATE OVERSIGHT BY REFUSING TO ANSWER EO 12333 QUESTIONS

The headlines from today's Senate Judiciary Committee hearing on NSA will no doubt be that Pat Leahy forced Keith Alexander to admit they've been lying about whether the 54 "plots" they "thwarted" were really "plots" or "thwarted" in the first place. Perhaps just two were.

More astute reporters might note that, in

response to questions about the NYT's report on the dossiers created in the course of foreign intelligence collection analysis, Keith Alexander offered several equivocations first claiming NYT got things wrong, then realizing that was a too broad claim. More interesting, he ultimately admitted that the NSA conducts some of this under Executive Order 12333 — the collection David Kris outlined in his paper.

There was even some follow-up on the NSA's use of EO 12333, with James Clapper and Alexander claiming Congress had some oversight of that collection (in spite of Dianne Feinstein's admission that they don't get news of EO 12333 violations even when they involve Americans).

But the most telling exchange occurred between Amy Klobuchar, Keith Alexander, and James Clapper. (after 1:25) Klobuchar asked why they hadn't told the Committee of the violations reported in an internal NSA review when they last appeared before the committee. After Alexander tried to filibuster (actually addressing the report in question and noting only ODNI and DOJ get those numbers, not FISC or Congress), Clapper interrupted and pretended she had asked about the LOVEINT incidents just reported to Charles Grassley. Clapper claimed those hadn't been reported because they were 12333 violations.

> Clapper: I think the answer to the question, Senator, was that the subject of the hearing was 215 and 702, and these 12 violations over 10 occurred under the foreign collection under the auspices of Executive Order 12333. [Sits back]
>
> Klobuchar: I thought we were broadly asking questions and it would have been nice to have heard about it there but it's behind us now.

But Clapper is absolutely incorrect. The review Klobuchar asked about reported 195 FISA

violations. Of those, 20% were due diligence violations — of an analyst not following Standard Operating Procedures she has been trained on. 31% are what amount to insufficient intelligence (these are called "resource violations"), resulting in searches on targets who shouldn't be targeted. A number of the incidents included not detasking someone quickly enough.

In other words, while this may (or may not) be minor, they are real violations of FISA authorities, the stuff that Congress and the Courts are supposed to oversee. And Clapper just blew off the question by saying they don't have to disclose any violations pertaining to EO 12333 (even though a chunk of these violations weren't EO 12333 violations).

Which of course demonstrates a further point. The Intelligence Community is basically refusing to discuss any EO 12333 violations and/or programs, even while it also picks up US person information at least incidentally.

And yet they claimed there was adequate oversight over those programs.

HAS FEDERAL USE OF DRONES VIOLATED EO 12333?

The Privacy and Civil Liberties Oversight Board just sent a letter to Eric Holder and James Clapper requesting that they have all the Intelligence Committee agencies update what are minimization procedures (though the letter doesn't call them that), "to take into account new developments including technological developments."

> As you know, Executive Order 12333

> establishes the overall framework for the conduct of intelligence activities by U.S. intelligence agencies. Under section 2.3 of the Executive Order, intelligence agencies can only collect, retain, and disseminate information about U.S. persons if the information fits within one of the enumerated categories under the Order and if it is permitted under that agency's implementing guidelines approved by the Attorney General after consultation with the Director of National Intelligence.
>
> The Privacy and Civil Liberties Oversight Board has learned that key procedures that form the guidelines to protect "information concerning United States person" have not comprehensively been updated, in some cases in almost three decades, despite dramatic changes in information use and technology.

The whole letter reads like the public record of a far more extensive and explicit classified discussion. Which makes me wonder what PCLOB found, in particular.

There are many technological issues that might be at issue – especially location data, but also generally Internet uses. Then there's the advance in database technology, making the sharing of information much more invasive because of the way it can be used. But I wonder if this letter isn't a demand that members of the intelligence community correct their use of drones.

The letter seems to point to something in EO 12333 Section 2.3 as its concern. Among the other potential enumerated categories of interest is this one:

> Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in

> accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. Those procedures shall permit collection, retention and dissemination of the following types of information:
>
> [snip]
>
> (h) Information acquired by overhead reconnaissance **not directed at specific United States persons**; [my emphasis]

We recently learned that the FBI has used drones in the following situations:

> UAVs have been used for surveillance to support missions related to kidnappings, search and rescue operations, drug interdictions, and fugitive investigations. Since late 2006, the FBI has conducted surveillance using UAVs in eight criminal cases and two national security cases. For example, earlier this year in Alabama, the FBI used UAV surveillance to support the successful rescue of the 5-year-old child who was being held hostage in an underground bunker by Jimmy Lee Dykes.
>
> [snip]
>
> The FBI does not use UAVs to conduct "bulk" surveillance or to conduct general surveillance not related to an investigation or an assessment.

It goes on to cite the Domestic Investigations and Operations Guide as its internal authority for the use of drones.

And while FBI's use of drones to catch a kidnapper may not fall under the FBI's intelligence mandate (and therefore may not violate EO 12333, which is about intelligence collection), it seems the two national security

uses would.

If the subject of those national security investigations was a US person, it would seem to be a violation of EO 12333.

Note, too, that drones are listed among PCLOB's focus items (see page 13).

That's just a guess. I would also imagine that minimization procedures need updated given the more prevalent use of databases (NCTC's access of government databases is another of PCLOB's focuses). I would imagine that some intelligence community members (including both the NCTC and DHS) are in violation of the mandate that the FBI collect foreign intelligence within the US. And PCLOB also cites GPC use as another of its foci, which is one of the technologies that has developed in the last 30 years.

But given the timing of it all, I wonder if this is a push to get the FBI to stop using drones for intelligence collection.