THE CORPORATE STORE: WHERE NSA GOES TO SHOP YOUR CONTENT AND YOUR LIFESTYLE

I'm increasingly convinced that for seven months, we've been distracted by a shiny object, the phone dragnet, the database recording all or almost all of the phone-based relationships in the US over the last five years. We were never wrong to discuss the dangers of the dragnet. It is the equivalent of a nuclear bomb, just waiting to go off. But I'm quite certain the NatSec establishment decided in the days after Edward Snowden's leaks to intensify focus on the actual construction of the dragnet — the collection of phone records and the limits on access to the initial database (what they call the collection store) of them — to distract us away from the true family jewels.

A shiny object.

All that time, I increasingly believe, we should have been talking about the corporate store, the database where queries from the collection store are kept for an undisclosed (and possibly indefinite) period of time. Once records get put in that database, I've noted repeatedly, they are subject to "the full range of [NSA's] analytic tradecraft."

We don't know precisely when that tradecraft gets applied or to how many of the phone identifiers collected in any given query. But we know that tradecraft includes matching individuals' various communication identifiers (which can include phone number, handset identifier, email address, IP address, cookies from various websites) — a process the NSA suggests may not be all that accurate, but whatever! Once NSA links all those identities, NSA can pull together both network maps and additional lifestyle information.

> The agency was authorized to conduct "large-scale graph analysis on very large sets of communications metadata without having to check foreignness" of every e-mail address, phone number or other identifier, the document said.
>
> [snip]
>
> The agency can augment the communications data with material from public, commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information, as well as property records and unspecified tax data, according to the documents. They do not indicate any restrictions on the use of such "enrichment" data, and several former senior Obama administration officials said the agency drew on it for both Americans and foreigners.

That analysis might even include tracking a person's online sex habits, if the government deems you a "radicalizer" for opposing unchecked US power, even if you're a US person.

Such profiles are not the only thing included in NSA's "full range of analytic tradecraft."

We also know — because James Clapper told us this very early on in this process — the metadata helps the NSA pick and locate which content to read. The head of NSA's Signals Intelligence Division, Theresa Shea, said this more plainly in court filings last year.

> Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links

> that have the highest probability of connection to terrorist targets. Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

The NSA prioritizes reading the content that involves US persons. And the NSA finds it, and decides what to read, using the queries that get dumped into the corporate store (presumably, they do some analytical tradecraft to narrow down which particular conversations involving US persons they want to read).

And there are several different kinds of content this might involve: content (phone or Internet) of a specific targeted individual — perhaps the identifier NSA conducted the RAS query with in the first place — already sitting on some NSA server, Internet and in some cases phone content the NSA can go get from providers after having decided it might be interesting, or content the NSA collects in bulk from upstream collections that was never targeted at a particular user.

The NSA is not only permitted to access all of this to see what Americans are saying, but in all but the domestically collected upstream content, it can go access the content by searching on the US person identifier, not the foreign interlocutor, without establishing even Reasonable Articulable Suspicion that it pertains to terrorism (though the analyst does have to claim it serves foreign intelligence purpose). That's important because lots of this

content-collection is not tied to a specific terrorist suspect (it can be tied to a geographical area, for example), so the NSA can hypothetically get to US person content without ever having reason to believe it has any tie to terrorism.

In other words, all the things NSA's defenders have been insisting the dragnet doesn't do — it doesn't provide content, it doesn't allow unaudited searches, NSA doesn't know identities, NSA doesn't data mine it, NSA doesn't develop dossiers on it, even James Clapper's claim that NSA doesn't voyeuristically troll through people's porn habits — every single one is potentially true for the results of queries run three hops off an identifier with just Reasonable Articulable Suspicion of some tie to terrorism (or Iran). Everything the defenders say the phone dragnet is not, the corporate store is.

All the phone contacts of all the phone contacts of all the phone contacts of someone subjected to the equivalent of a digital stop-and-frisk are potentially subject to all the things NSA's defenders assure us the dragnet is not subject to.

Don't get me wrong: I'm not saying some of this analysis isn't appropriate with actual terrorist suspects.

But that's not what the corporate store is. It is — PCLOB estimates — up to 120 million phone users (the actual number of people would be smaller because of burner phones, and a significant number would be foreign numbers), the overwhelming majority of which are completely innocent of anything but being up to 3 degrees away from a guy who got digitally stop-and-frisked.

Yet those potentially millions of Americans get no effective protection once they're in the corporate store. As the PCLOB elaborates,

> Once contained in the corporate store, analysts may further examine these

> records without the need for any new reasonable articulable suspicion determination.
>
> [snip]
>
> Furthermore, under the rules approved by the FISA court, NSA personnel may then search any phone number, including the phone number of a U.S. person, against the corporate store — as long as the agency has a valid foreign intelligence purpose in doing so — without regard to whether there is "reasonable articulable suspicion" about that number. 589 Unlike with respect to the initial RAS query, the FISA court's orders specifically exempt the NSA from maintaining an audit trail when analysts access records in the corporate store. 590

There are just a few protections. The analysts accessing the corporate store need to have undergone training and must claim a foreign intelligence (but not exclusively counterterrorism) purpose. And normally, if NSA wants to circulate the US person data outside of the NSA, a high level official must certify that,

> the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.

Again, that doesn't require the US person have any tie to counterterrorism, just that it be "related to" counterterrorism, which FISC has already deemed even the larger collection store to be by default. (The Executive Branch can also search the corporate store for exculpatory or inculpatory information, which, given that no defendant has succeeded in getting a search for the former, probably means it is only used for

the latter — and note, this is not, apparently, limited to counterterrorism purposes, and as of right now the Executive is also permitted to do back door searches of content for criminal evidence unrelated to terrorism, though Obama has vaguely promised to change that while stopping short of a warrant.)

And no one, aside from PCLOB's estimate of up to 120 million (which may or may not have been reviewed when PCLOB let the IC review some of their process descriptions), is talking about how many Americans are in the corporate store. Geoffrey Stone has said NSA only "touched" 6,000 people in 2012, though that may mean only 6,000 of a much larger number of people who got placed in the corporate store were subjected to further NSA processing. We can assume the numbers were far higher until 2009, when there were over 17,000 on a RAS list. Furthermore, I'm very curious to see whether such numbers spike for 2013, given claims that NSA used the dragnet for "peace of mind" after the Boston Marathon attack, launched by young men who interacted via mobile phone with a huge number of totally innocent US person contacts. Will half of Cambridge, MA be subject to the full range of NSA's tradecraft because we used the dragnet to get peace of mind after the Boston Marathon attack?

Moreover, as discussed last month, the NSA can alter the intake into the corporate store via choices made by data integrity analysts — the other part of the process largely exempted from oversight, and with a few inclusions could cause the bulk of American call records to end up in the corporate store.

Obama said the dragnet "does not involve the NSA examining the phone records of ordinary Americans." But in doing so, he was implying that the millions of Americans whose records may have made it into the corporate store are not ordinary, and therefore not entitled to the kind of due process enshrined in the Constitution.

PCLOB ESTIMATES 120 MILLION PHONE NUMBERS IN CORPORATE STORE

PCLOB's report confirms something ACLU's Patrick Toomey and I have been harping on. One of the biggest risks of the phone dragnet stems not from the initial queries themselves, but from NSA's storage of query results in the "corporate store," permanently, where they can be accessed without the restrictions required for access to the full database, and exposed to all the rest of NSA's neat toys.

> According to the FISA court's orders, records that have been moved into the corporate store may be searched by authorized personnel "for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms."71 Analysts therefore can query the records in the corporate store with terms that are not reasonably suspected of association with terrorism. They also are permitted to analyze records in the corporate store through means other than individual contact-chaining queries that begin with a single selection term: because the records in the corporate store all stem from RAS-approved queries, the agency is allowed to apply other analytic methods and techniques to the query results.72 For instance, such calling records may be integrated with data acquired under other authorities for further analysis. The FISA court's orders expressly state that the NSA may apply "the full range" of signals intelligence analytic tradecraft to the

> calling records that are responsive to a query, which includes every record in the corporate store.73

PCLOB doesn't say it, but NSA's SID Director Theresa Shea has: those other authorities include content collection, which means coming up in a query can lead directly to someone reading your content.

> Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

Plus, those authorities will include datamining, including with other data collected by NSA, like a user's Internet habits and financial records.

Then, PCLOB does some math to estimate how many numbers might be in the corporate store.

> If a seed number has seventy-five direct contacts, for instance, and each of these first-hop contact has seventy-five

> new contacts of its own, then each query would provide the government with the complete calling records of 5,625 telephone numbers. And if each of those second-hop numbers has seventy-five new contacts of its own, a single query would result in a batch of calling records involving over 420,000 telephone numbers.
>
> [snip]
>
> If the NSA queries around 300 seed numbers a year, as it did in 2012, then based on the estimates provided earlier about the number of records produced in response to a single query, the corporate store would contain records involving over 120 million telephone numbers.74
>
> 74 While fewer than 300 identifiers were used to query the call detail records in 2012, that number "has varied over the years." Shea Decl. ¶ 24.

Some might quibble with these numbers: other estimates use 40 contacts per person (though remember, there's 5 years of data), and the estimate doesn't seem to account for mutual contacts. Plus, remember this is unique phone numbers: we should expect it to include fewer people, because people — especially people trying to hide — change phones regularly. Further, remember a whole lot of foreign numbers will be in there.

But other things suggest it might be conservative. As a recent Stanford study showed, if the NSA isn't really diligent about removing high volume numbers, then queries could quickly include everyone; certainly, NSA could have deliberately populated the corporate store by leaving such identifiers in. We know there were 27,000 people cleared for RAS in 2008 and 17,000 on an alert list in 2009, meaning the query numbers for earlier years are effectively much

much higher (which seems to be the point of footnote 74).

Plus, remember that PCLOB gave their descriptive sections to the NSA to review for accuracy. So I assume NSA did not object to the estimate.

So 120 million phone numbers might be a reasonable estimate.

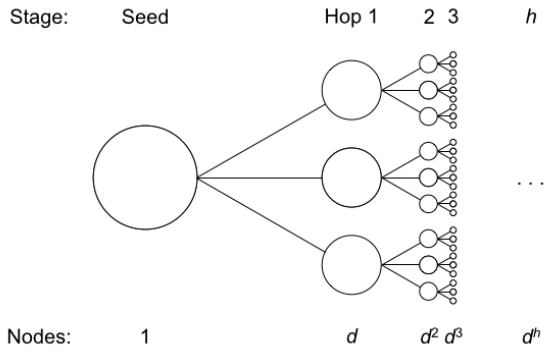
That's a lot of Americans exposed to the level of data analysis permissible in the corporate store.

THREE-HOPPING THE CORPORATE STORE, IN THEORY

Stanford University has been running a project to better understand what phone metadata can show about users, MetaPhone, in which Android users can make their metadata available for analysis.

They just published a piece that suggests we could be underestimating the intrusiveness of the government's phone dragnet program. That's because most assumptions about degrees of separation consider only human contacts, and not certain hub phone numbers that quickly unite us.

> A common approach for calculating these figures has been to simply assume an average number of call relationships per phone line ("degree"), then multiply out the number of hops. If a single phone number has average degree d, and the NSA can make h hops, then a single query gives expected access to
>
> about d^h complete sets of phone
>
> records.[3, 4]



> *We turned to our crowdsourced MetaPhone dataset for an empirical measurement. Given our small, scattershot, and time-limited sample of phone activity, we expected our graph to be largely disconnected. After all, just one pair from our hundreds of participants had held a call.*

> Surprisingly, our call graph *was* connected. Over 90% of participants were related in a single graph component. And within that component, participants were closely linked: on average, over 10% of participants were just 2 hops away, and over 65% of participants were 4 or fewer hops away!

In spite of the fact that just 2 of its participants had called each other, the fact that so many people had called TMobile's voicemail number connected 17% of participants at two hops.

> Already 17.5% of participants are linked. That makes intuitive sense—many Americans use T-Mobile for mobile phone service, and many call into voicemail. Now think through the magnitude of the privacy impact: T-Mobile has over 45 million subscribers in the United

> States. That's potentially tens of millions of Americans connected by just two phone hops, solely because of how their carrier happens to configure voicemail.

And from this, the piece concludes that NSA could get access to a huge number of numbers with just one seed.

> But our measurements are highly suggestive that many previous estimates of the NSA's three-hop authority were conservative. Under current FISA Court orders, the NSA may be able to analyze the phone records of a sizable proportion of the United States population with just one seed number.

This analysis doesn't account for one thing: NSA uses Data Integrity Analysts who take out high volume numbers — numbers like the TMobile voice mail number.

Here's how the 2009 End-to-End review of the phone dragnet described their role.

> As part of their Court-authorized function of ensuring BR FISA metadata is properly formatted for analysis, Data Integrity Analysts seek to identify numbers in the BR FISA metadata that are not associated with specific users, e.g., "high volume identifiers." [Entire sentence redacted] NSA determined during the end-to-end review that the Data Integrity Analysts' practice of populating non-user specific numbers in NSA databases had not been described to the Court.
>
> (TS//SI//NT) For example, NSA maintains a database, [redacted] which is widely used by analysts and designed to hold identifiers, to include the types of non-user specific numbers referenced above, that, based on an analytic

> judgment, should not be tasked to the SIGINT system. In an effort to help minimize the risk of making incorrect associations between telephony identifiers and targets, the Data Integrity Analysts provided [redacted] included in the BR metadata to [redacted] A small number of [redacted] BR metadata numbers were stored in a file that was accessible by the BR FISA-enabled [redacted], a federated query tool that allowed approximately 200 analysts to obtain as much information as possible about a particular identifier of interest. Both [redacted] and the BR FISA-enabled [redacted] allowed analysts outside of those authorized by the Court to access the non-user specific number lists.
>
> In January 2004, [redacted] engineers developed a "defeat list" process to identify and remove non-user specific numbers that are deemed to be of little analytic value and that strain the system's capacity and decrease its performance. In building defeat lists, NSA identified non-user specific numbers in data acquired pursuant to the BR FISA Order as well as in data acquired pursuant to EO 12333. Since August 2008, [redacted] had also been sending all identifiers on the defeat list to the [several lines redacted].

And here's a (heavily-redacted) training module that describes what kind of massaging the tech people (which is a wider set of people than just the Data Integrity Analysts) do with dragnet data.

If the Data Integrity Analysts operate as multiple NSA documents say they do, this kind of quick inclusion of all Americans shouldn't happen — it's precisely the kind of noise NSA says it is trying to defeat.

There are just two problems with this then. First, as I have noted in the past, the inclusion or exclusion of high volume numbers will at times be a judgment call, and could lead to eliminating the most valuable pieces of intelligence in the dataset if targets knowingly or unknowingly exploit these high volume numbers. Similarly, it could easily be used — and may already have been — to make the dragnets totally unusable at critical times.

More importantly, this tech role receives far less oversight than the regular analysts do. And Dianne Feinstein's Fake FISA Fix might even eliminate some of the oversight on the position now. So we have almost no way (and Congress seems to want to deprive itself of having a way) of ensuring these Data Integrity Analysts are doing what we think they're doing.

If NSA is doing what it says, then the Stanford analysis should be moot, because it doesn't account for that Data Integrity role. But ACLU's Patrick Toomey explained back in August, NSA has a very real incentive to get as much data picked up in queries and into the corporate store as it can.

> All of this information, the primary order says, is dumped into something called the "corporate store." Incredibly, the FISC imposes *no* restrictions on what analysts may subsequently do with the information. The FISC's primary order contains a crucially revealing footnote stating that "the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the result of intelligence analysis queries of the collected [telephone] metadata." In short, once a calling record is added to the corporate store, anything goes.
>
> More troubling, if the government is combining the results of *all* its queries in this "corporate store," as seems likely, then it has a massive pool of

> telephone data that it can analyze in any way it chooses, unmoored from the specific investigations that gave rise to the initial queries. To put it in individual terms: If, for some reason, your phone number happens to be within three hops of an NSA target, *all* of your calling records may be in the corporate store, and thus available for any NSA analyst to search at will.
>
> But it's even worse than that. The primary order prominently states that whenever the government accesses the wholesale telephone-metadata database, "an auditable record of the activity shall be generated." It might feel fairly comforting to know that, if the government abuses its access to all Americans' call data, it might eventually be called to account—until you read footnote 6 of the primary order, which *exempts entirely* the government's use of the "corporate store" from the audit-trail requirement.

Not "defeating" numbers like the TMobile voice mail is a very easy way to populate the corporate store with very very broad swaths of US person data so as to be able to access it with much less stringent controls.

All of which demonstrates the urgency for more oversight into whether the Data Integrity Analysts are doing what they say they're doing.

A DRAGNET OF EMPTYWHEEL'S MOST

IMPORTANT POSTS ON SURVEILLANCE, 2007 TO 2017

Happy Birthday to me! To us! To the emptywheel community!

On December 3, 2007, emptywheel first posted as a distinct website. That makes us, me, we, ten this week.

To celebrate, the emptywheel team has been sharing some of our favorite work from the last decade. This is my massive dragnet of surveillance posts.

For years, we've done this content ad free, relying on donations and me doing freelance work for others to fund the stuff you read here. I would make far more if I worked for some free-standing outlet, but I wouldn't be able to do the weedy, iterative work that I do here, which would amount to not being able to do my best work.

If you've found this work valuable — if you'd like to ensure it remains available for the next ten years — please consider supporting the site.

2007

Whitehouse Reveals Smoking Gun of White House Claiming Not to Be Bound by Any Law

Just days after opening the new digs, I noticed Sheldon Whitehouse entering important details into the Senate record — notably, that John Yoo had pixie dusted EO 12333 to permit George Bush to authorize the Stellar Wind dragnet. In the ten years since, both parties worked to

gradually expand spying on Americans under EO 12333, only to have Obama permit the sharing of raw EO 12333 data in its last days in office, completing the years long project of restoring Stellar Wind's functionalities. This post, from 2016, analyzes a version of the underlying memo permitting the President to change EO 12333 without providing public notice he had done so.

2008

McConnell and Mukasey Tell Half Truths

In the wake of the Protect America Act, I started to track surveillance legislation as it was written, rather than figure out after the fact how the intelligence community snookered us. In this post, I examined the veto threats Mike McConnell and Michael Mukasey issued in response to some Russ Feingold amendments to the FISA Amendments Act and showed that the government intended to use that authority to access Americans' communication via both what we now call back door searches and reverse targeting. "That is, one of the main purposes is to collect communications in the United States."

9 years later, we're still litigating this (though, since then FISC has permitted the NSA to collect entirely domestic communications under the 2014 exception).

2009

FISA + EO 12333 + [redacted] procedures = No Fourth Amendment

The Government Sez: We Don't Have a Database of All Your Communication

After the FISCR opinion on what we now know to be the Yahoo challenge to Protect American Act first got declassified, I identified several issues that we now have much more visibility on. First, PAA permitted spying on Americans overseas under EO 12333. And it didn't achieve particularity through the PAA, but instead through what we know to be targeting procedures, including contact chaining. Since then we've learned the role of SPCMA in this.

In addition, to avoid problems with back door searches, the government claimed it didn't have a database of all our communication — a claim that, narrowly parsed might be true, but as to the intent of the question was deeply misleading. That claim is one of the reasons we've never had a real legal review of back door searches.

Bush's Illegal Domestic Surveillance Program and Section 215

On PATRIOTs and JUSTICE: Feingold Aims for Justice

During the 2009 PATRIOT Act reauthorization, I continued to track what the government hated most as a way of understanding what Congress was really authorizing. I understood that Stellar Wind got replaced not just by PAA and FAA, but also by the PATRIOT authorities.

> All of which is a very vague way to say

> we probably ought to be thinking of four programs—Bush's illegal domestic surveillance program and the PAA/FAA program that replaced it, NSLs, Section 215 orders, and trap and trace devices—as one whole. As the authorities of one program got shut down by exposure or court rulings or internal dissent, it would migrate to another program. That might explain, for example, why Senators who opposed fishing expeditions in 2005 would come to embrace broadened use of Section 215 orders in 2009.

I guessed, for example, that the government was bulk collecting data and mining it to identify targets for surveillance.

> We probably know what this is: the bulk collection and data mining of information to select targets under FISA. Feingold introduced a bajillion amendments that would have made data mining impossible, and each time Mike McConnell and Michael Mukasey would invent reasons why Feingold's amendments would have dire consequences if they passed. And the legal information Feingold refers to is probably the way in which the Administration used EO 12333 and redacted procedures to authorize the use of data mining to select FISA targets.

Sadly, I allowed myself to get distracted by my parallel attempts to understand how the government used Section 215 to obtain TATP precursors. As more and more people confirmed that, I stopped pursuing the PATRIOT Act ties to 702 as aggressively.

2010

Throwing our PATRIOT at Assange

This may be controversial, given everything that has transpired since, but it is often forgotten what measures the US used against Wikileaks in 2010. The funding boycott is one thing (which is what led Wikileaks to embrace Bitcoin, which means it is now in great financial shape). But there's a lot of reason to believe that the government used PATRIOT authorities to target not just Wikileaks, but its supporters and readers; this was one hint of that in real time.

2011

The March–and April or May–2004 Changes to the Illegal Wiretap Program

When the first iteration of the May 2004 Jack Goldsmith OLC memo first got released, I identified that there were multiple changes made and unpacked what some of them were. The observation that Goldsmith newly limited Stellar Wind to terrorist conversations is one another reporter would claim credit for "scooping" years later (and get the change wrong in the process). We're now seeing the scope of targeting morph again, to include a range of domestic crimes.

Using Domestic Surveillance to Get Rapists to Spy for America

Something that is still not widely known about 702 and our other dragnets is how they are used to identify potential informants. This post, in which I note Ted Olson's 2002 defense of using

(traditional) FISA to find rapists whom FBI can then coerce to cooperate in investigations was the beginning of my focus on the topic.

2012

FISA Amendments Act: "Targeting" and "Querying" and "Searching" Are Different Things

During the 2012 702 reauthorization fight, Ron Wyden and Mark Udall tried to stop back door searches. They didn't succeed, but their efforts to do so revealed that the government was doing so. Even back in 2012, Dianne Feinstein was using the same strategy the NSA currently uses — repeating the word "target" over and over — to deny the impact on Americans.

Sheldon Whitehouse Confirms FISA Amendments Act Permits Unwarranted Access to US Person Content

As part of the 2012 702 reauthorization, Sheldon Whitehouse said that requiring warrants to access the US person content collected incidentally would "kill the program." I took that as confirmation of what Wyden was saying: the government was doing what we now call back door searches.

2013

20 Questions: Mike Rogers' Vaunted Section 215 Briefings

After the Snowden leaks started, I spent a lot of time tracking bogus claims about oversight. After having pointed out that, contrary to Administration claims, Congress did not have the opportunity to be briefed on the phone dragnet before reauthorizing the PATRIOT Act in 2011, I then noted that in one of the only briefings available to non-HPSCI House members, FBI had lied by saying there had been no abuses of 215.

John Bates' TWO Wiretapping Warnings: Why the Government Took Its Internet Dragnet Collection Overseas

Among the many posts I wrote on released FISA orders, this is among the most important (and least widely understood). It was a first glimpse into what now clearly appears to be 7 years of FISA violation by the PRTT Internet dragnet. It explains why they government moved much of that dragnet to SPCMA collection. And it laid out how John Bates used FISA clause 1809(a)(2) to force the government to destroy improperly collected data.

Federated Queries and EO 12333 FISC Workaround

In neither NSA nor FBI do the authorities work in isolation. That means you can conduct a query

on federated databases and obtain redundant results in which the same data point might be obtained via two different authorities. For example, a call between Michigan and Yemen might be collected via bulk collection off a switch in or near Yemen (or any of the switches between there and the US), as well as in upstream collection from a switch entering the US (and all that's assuming the American is not targeted). The NSA uses such redundancy to apply the optimal authority to a data point. With metadata, for example, it trained analysts to use SPCMA rather than PATRIOT authorities because they could disseminate it more easily and for more purposes. With content, NSA appears to default to PRISM where available, probably to bury the far more creative collection under EO 12333 for the same data, and also because that data comes in structured form.

Also not widely understood: the NSA can query across metadata types, returning both Internet and phone connection in the same query (which is probably all the more important now given how mobile phones collapse the distinction between telephony and Internet).

This post described how this worked with the metadata dragnets.

The Purpose(s) of the Dragnet, Revisited

The government likes to pretend it uses its dragnet only to find terrorists. But it does far more, as this analysis of some court filings lays out.

2014

The Corporate Store:

Where NSA Goes to Shop Your Content and Your Lifestyle

There's something poorly understood about the metadata dragnets NSA conducts. The contact-chaining isn't the point. Rather, the contact-chaining serves as a kind of nomination process that puts individuals' selectors, indefinitely, into the "corporate store," where your identity can start attracting other related datapoints like a magnet. The contact-chaining is just a way of identifying which people are sufficiently interesting to submit them to that constant, ongoing data collection.

SPCMA: The Other NSA Dragnet Sucking In Americans

I've done a lot of work on SPCMA — the authorization that, starting in 2008, permitted the NSA to contact chain on and through Americans with EO 12333 data, which was one key building block to restoring access to EO 12333 analysis on Americans that had been partly ended by the hospital confrontation, and which is where much of the metadata analysis affecting Americans has long happened. This was my first comprehensive post on it.

The August 20, 2008 Correlations Opinion

A big part of both FBI and NSA's surveillance involves correlating identities — basically, tracking all the known identities a person uses on telephony and the Internet (and financially, though we see fewer details of that), so as to be able to pull up all activities in one profile (what Bill Binney once called "dossiers"). It turns out the FISC opinion authorizing such

correlations is among the documents the government still refuses to release under FOIA. Even as I was writing the post Snowden was explaining how it works with XKeyscore.

A Yahoo! Lesson for USA Freedom Act: Mission Creep

This is another post I refer back to constantly. It shows that, between the time Yahoo first discussed the kinds of information they'd have to hand over under PRISM in August 2007 and the time they got directives during their challenge, the kinds of information they were asked for expanded into all four of its business areas. This is concrete proof that it's not just emails that Yahoo and other PRISM providers turn over — it's also things like searches, location data, stored documents, photos, and cookies.

FISCR Used an Outdated Version of EO 12333 to Rule Protect America Act Legal

Confession: I have an entire chapter of the start of a book on the Yahoo challenge to PRISM. That's because so much about it embodied the kind of dodgy practices the government has, at the most important times, used with the FISA Court. In this post, I showed that the documents that the government provided the FISCR hid the fact that the then-current versions of the documents had recently been modified. Using the active documents would have shown that Yahoo's key argument — that the government could change the rules protecting Americans anytime, in secret — was correct.

2015

Is CISA the Upstream Cyber Certificate NSA Wanted But Didn't Really Get?

Among the posts I wrote on CISA, I noted that because the main upstream 702 providers have a lot of federal business, they'll "voluntarily" scan on any known cybersecurity signatures as part of protecting the federal government. Effectively, it gives the government the certificate it wanted, but without any of the FISA oversight or sharing restrictions. The government has repeatedly moved collection to new authorities when FISC proved too watchful of its practices.

The FISA Court's Uncelebrated Good Points

Many civil libertarians are very critical of the FISC. Not me. In this post I point out that it has policed minimization procedures, conducted real First Amendment reviews, taken notice of magistrate decisions and, in some cases, adopted the highest common denominator, and limited dissemination.

How the Government Uses Location Data from Mobile Apps

Following up on a Ron Wyden breadcrumb, I figured out that the government – under both FISA and criminal law – obtain location data from mobile apps. While the government still has to adhere to the collection standard in any

given jurisdiction, obtaining the data gives the government enhanced location data tied to social media, which can implicate associates of targets as well as the target himself.

The NSA (Said It) Ate Its Illegal Domestic Content Homework before Having to Turn It in to John Bates

I'm close to being able to show that even after John Bates reauthorized the Internet metadata dragnet in 2010, it remained out of compliance (meaning NSA was *always* violating FISA in obtaining Internet metadata from 2002 to 2011, with a brief lapse). That case was significantly bolstered when it became clear NSA hastily replaced the Internet dragnet with obtaining metadata from upstream collection after the October 2011 upstream opinion. NSA hid the evidence of problems on intake from its IG.

FBI Asks for at Least Eight Correlations with a Single NSL

As part of my ongoing effort to catalog the collection and impact of correlations, I showed that the NSL Nick Merrill started fighting in 2004 asked for eight different kinds of correlations before even asking for location data. Ultimately, it's these correlations as much as any specific call records that the government appears to be obtaining with NSLs.

2016

What We Know about the Section 215 Phone Dragnet and Location Data

During the lead-up to the USA Freedom Debate, the government leaked stories about receiving a fraction of US phone records, reportedly because of location concerns. The leaks were ridiculously misleading, in part because they ignored that the US got redundant collection of many of exactly the same calls they were looking for from EO 12333 collection. Yet in spite of these leaks, the few figured out that the need to be able to force Verizon and other cell carriers to strip location data was a far bigger reason to pass USAF than anything Snowden had done. This post laid out what was known about location data and the phone dragnet.

While It Is Reauthorizing FISA Amendments Act, Congress Should Reform Section 704

When Congress passed FISA Amendments Act, it made a show of providing protections to Americans overseas. One authority, Section 703, was for spying on people overseas with help of US providers, and another was for spying on Americans overseas without that help. By May 2016, I had spent some time laying out that only the second, which has less FISC oversight, was used. And I was seeing problems with its use in reporting. So I suggested maybe Congress should look into that?

It turns out that at precisely that moment, NSA was wildly scrambling to get a hold on its 704 collection, having had an IG report earlier in

the year showing they couldn't audit it, find it all, or keep it within legal boundaries. This would be the source of the delay in the 702 reauthorization in 2016, which led to the prohibition on about searches.

The Yahoo Scan: On Facilities and FISA

The discussion last year of a scan the government asked Yahoo to do of all of its users was muddled because so few people, even within the privacy community, understand how broadly the NSA has interpreted the term "selector" or "facility" that it can target for collection. The confusion remains to this day, as some in the privacy community claim HPSCI's use of facility based language in its 702 reauthorization bill reflects *new* practice. This post attempts to explain what we knew about the terms in 2016 (though the various 702 reauthorization bills have offered some new clarity about the distinctions between the language the government uses).

2017

Ron Wyden's History of Bogus Excuses for Not Counting 702 US Person Collection

Ron Wyden has been asking for a count of how many Americans get swept up under 702 for years. The IC has been inventing bogus explanations for why they can't do that for years. This post chronicles that process and explains why the debate is so important.

The Kelihos Pen Register: Codifying an Expansive Definition of DRAS?

When DOJ used its new Rule 41 hacking warrant against the Kelihos botnet this year, most of the attention focused on that first-known usage. But I was at least as interested in the accompanying Pen Register order, which I believe may serve to codify an expansion of the dialing, routing, addressing, and signaling information the government can obtain with a PRTT. A similar codification of an expansion exists in the HJC and Lee-Leahy bills reauthorizing 702.

The Problems with Rosemary Collyer's Shitty Upstream 702 Opinion

The title speaks for itself. I don't even consider Rosemary Collyer's 2017 approval of 702 certificates her worst FISA opinion ever. But it is part of the reason why I consider her the worst FISC judge.

It Is False that Downstream 702 Collection Consists Only of To and From Communications

I pointed out a number of things not raised in a panel on 702, not least that the authorization of EO 12333 sharing this year probably replaces some of the "about" collection function. Most of all, though, I reminded that in spite of what often gets claimed, PRISM is far more than just

communications to and from a target.

UNITEDRAKE and Hacking under FISA Orders

A document leaked by Shadow Brokers reveals a bit about how NSA uses hacking on FISA targets. Perhaps most alarmingly, the same tools that conduct such hacks can be used to impersonate a user. While that might be very useful for collection purposes, it also invites very serious abuse that might create a really nasty poisonous tree.

A Better Example of Article III FISA Oversight: Reaz Qadir Khan

In response to Glenn Gerstell's claims that Article III courts have exercised oversight by approving FISA practices (though the reality on back door searches is not so cut and dry), I point to the case of Reaz Qadir Khan where, as Michael Mosman (who happens to serve on FISC) moved towards providing a CIPA review for surveillance techniques, Khan got a plea deal.

The NSA's 5-Page Entirely Redacted Definition of Metadata

In 2010, John Bates redefined metadata. That five page entirely redacted definition became codified in 2011. Yet even as Congress moves to reauthorize 702, we don't know what's included in that definition (note: location would be included).

FISA and the Space-Time Continuum

This post talks about how NSA uses its various authorities to get around geographical and time restrictions on its spying.

The Senate Intelligence Committee 702 Bill Is a Domestic Spying Bill

This is one of the most important posts on FISA I've ever written. It explains how in 2014, to close an intelligence gap, the NSA got an exception to the rule it has to detask from a facility as soon as it identifies Americans using the facility. The government uses it to collect on Tor and, probably VPN, data. Because the government can keep entirely domestic communications that the DIRNSA has deemed evidence of a crime, the exception means that 702 has become a domestic spying authority for use with a broad range of crimes, not to mention anything the Attorney General deems a threat to national security.

"Hype:" How FBI Decided Searching 702 Content Was the Least Intrusive Means

In a response to a rare good faith defense of FBI's back door searches, I pointed out that the FBI is obliged to consider the least intrusive means of investigation. Yet, even while it admits that accessing content like that obtained via 702 is extremely intrusive, it nevertheless uses the technique routinely at the assessment level.

Other Key Posts Threads

10 Years of emptywheel: Key Non-Surveillance Posts 2008-2010

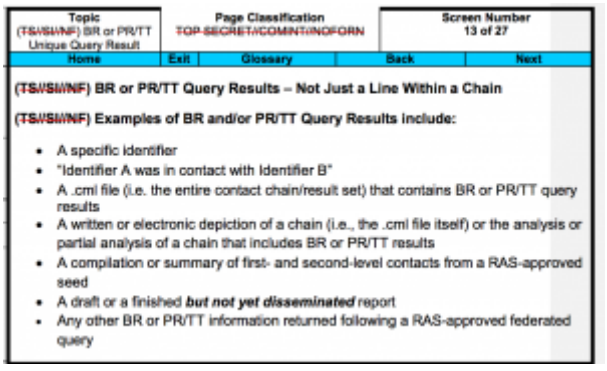
10 Years of emptywheel: Key Non-Surveillance Posts 2011-2012

10 Years of emptywheel: Key Non-Surveillance Posts 2013-2015

10 Years of emptywheel: Key Non-Surveillance Posts 2016-2017

10 Years of emptywheel: Jim's Dimestore

ANOTHER PROBABLE REASON TO SHUT DOWN THE INTERNET DRAGNET: DISSEMINATION RESTRICTIONS


Topic
(TS//SI//NF) BR or PR/TT Unique Query Result

Page Classification
TOP SECRET//COMINT//NOFORN

Screen Number
13 of 27

Home | Exit | Glossary | Back | Next

(TS//SI//NF) BR or PR/TT Query Results – Not Just a Line Within a Chain

(TS//SI//NF) Examples of BR and/or PR/TT Query Results include:

- A specific identifier
- "Identifier A was in contact with Identifier B"
- A .cmf file (i.e. the entire contact chain/result set) that contains BR or PR/TT query results
- A written or electronic depiction of a chain (i.e., the .cmf file itself) or the analysis or partial analysis of a chain that includes BR or PR/TT results
- A compilation or summary of first- and second-level contacts from a RAS-approved seed
- A draft or a finished ***but not yet disseminated*** report
- Any other BR or PR/TT information returned following a RAS-approved federated query

I noted the other day that an NSA IG document liberated by Charlie Savage shows the agency had 4 reasons to shut down the domestic Internet (PRTT) dragnet, only one of which is the publicly admitted reason — that NSA could accomplish what it needed to using SPCMA and FAA collection.

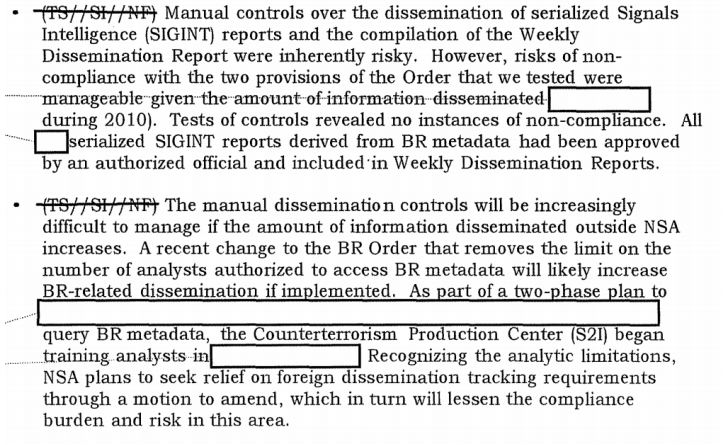
I'm fairly sure another of the reasons NSA shut down the dragnet is because of dissemination restrictions that probably got newly reinvigorated in mid-2011.

I laid out a timeline of events leading up to the shutdown of the Internet dragnet here. I've added one date: that of the draft training program, several modules of which are dated October 17, 2011, released under FOIA (given other dates in the storyboard, the program had clearly been in development as early as November 2010). How odd is that? The NSA was just finalizing a training program on the Internet (and phone) dragnet as late as 6 weeks before NSA hastily shut it down starting in late November 2011. The training program — which clearly had significant Office of General Counsel involvement — provides a sense of what compliance issues OGC was emphasizing just as NSA decided to shut down the Internet dragnet.

The training program was done in the wake of two things: a series of audits mandated by the FISA Court (see PDF 36) that lasted from May 2010 until early 2011, and the resumption of the PRTT Internet dragnet between July and October 2010.

The series of audits revealed several things. First, as I have long argued was likely, the technical personnel who monitor the data for integrity may also use their access to make inappropriate queries, as happened in an incident during this period (see PDF 95 and following); I plan to return to this issue. In addition, at the beginning of the period — before a new selector tracking tool got introduced in June 2010 — NSA couldn't track whether some US person selectors had gotten First Amendment review. And, throughout the audit period, the IG simply didn't review whether less formalized disseminations of dragnet results followed the rules, because it was too hard to audit. The final report summarizing the series of audits from May 2011 (as well as the counterpart one covering the Internet dragnet) identified this as one of the

weaknesses of the program, but NSA wanted to manage it by just asking FISC to eliminate the tracking requirements for foreign selectors (see PDF 209).

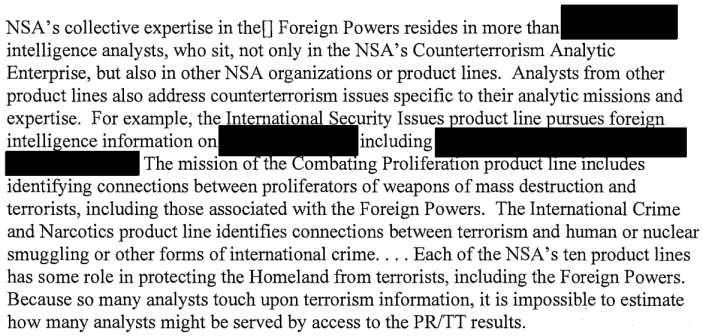


- ~~(TS//SI//NF)~~ Manual controls over the dissemination of serialized Signals Intelligence (SIGINT) reports and the compilation of the Weekly Dissemination Report were inherently risky. However, risks of non-compliance with the two provisions of the Order that we tested were manageable given the amount of information disseminated [redacted] during 2010). Tests of controls revealed no instances of non-compliance. All [redacted] serialized SIGINT reports derived from BR metadata had been approved by an authorized official and included in Weekly Dissemination Reports.

- ~~(TS//SI//NF)~~ The manual dissemination controls will be increasingly difficult to manage if the amount of information disseminated outside NSA increases. A recent change to the BR Order that removes the limit on the number of analysts authorized to access BR metadata will likely increase BR-related dissemination if implemented. As part of a two-phase plan to [redacted] query BR metadata, the Counterterrorism Production Center (S2I) began training analysts in [redacted] Recognizing the analytic limitations, NSA plans to seek relief on foreign dissemination tracking requirements through a motion to amend, which in turn will lessen the compliance burden and risk in this area.

I found this blasé attitude about dissemination remarkable given that in June 2009, Reggie Walton had gotten furious with NSA for not following dissemination restrictions, after which NSA did it again in September 2009, and didn't tell Walton about it, which made him furious all over again. Dissemination restrictions were something Walton had made clear he cared about, and NSA IG's response was simply to say auditing for precisely the kind of thing he was worried about — informal dissemination — was too hard, so they weren't going to do it, not even for the audits FISC (probably Walton himself) ordered NSA to do to make sure they had cleaned up all the violations discovered in 2009.

Meanwhile, when NSA got John Bates to authorize the resumption of the dragnet (he signed the order in July 2010, but it appears it didn't resume in earnest until October 2010), they got him to approve the dissemination of PRTT data broadly within NSA. This was a response to a Keith Alexander claim, made the year before, that all product lines within NSA might have a role in protecting against terrorism (see PDF 89).



NSA's collective expertise in the[] Foreign Powers resides in more than [redacted] intelligence analysts, who sit, not only in the NSA's Counterterrorism Analytic Enterprise, but also in other NSA organizations or product lines. Analysts from other product lines also address counterterrorism issues specific to their analytic missions and expertise. For example, the International Security Issues product line pursues foreign intelligence information on [redacted] including [redacted] The mission of the Combating Proliferation product line includes identifying connections between proliferators of weapons of mass destruction and terrorists, including those associated with the Foreign Powers. The International Crime and Narcotics product line identifies connections between terrorism and human or nuclear smuggling or other forms of international crime. . . . Each of the NSA's ten product lines has some role in protecting the Homeland from terrorists, including the Foreign Powers. Because so many analysts touch upon terrorism information, it is impossible to estimate how many analysts might be served by access to the PR/TT results.

In other words, even as NSA's IG was deciding it couldn't audit for informal dissemination because it was too hard to do (even while acknowledging that was one of the control weaknesses of the program), NSA asked for and got FISC to expand dissemination, at least for the Internet dragnet, to basically everyone. (The two dragnets appear to have been synched again in October 2010, as they had been for much of 2009, and when that happened the NSA asked for all the expansions approved for the Internet dragnet to be applied to the phone dragnet.)

Which brings us to the training program.

There are elements of the training program that reflect the violations of the previous years, from an emphasis on reviewing for access restrictions to a warning that tech personnel should only use their sysadmin access to raw data for technical purposes, and not analytical ones.

But the overwhelming emphasis in the training was on dissemination — which is a big part of the reason the NSA used the program to train analysts to rerun PATRIOT-authorized queries under EO 12333 so as to bypass dissemination restrictions. As noted in the screen capture above, the training program gave a detailed list of the things that amounted to dissemination, including oral confirmation that two identifiers — even by name (which of course confirms that these phone numbers are identifiable to analysts) — were in contact.

> In addition, any summary of that information would also be a BR or PR/TT query result. So, if you knew that

> identifier A belonged to Joe and identifier B belonged to Sam, and the fact of that contact was derived from BR or PR/TT metadata, if you communicate orally or in writing that Joe talked to Sam, even if you don't include the actual e-mail account or telephone numbers that were used to communicate, this is still a BR or PR/TT query result.

The program reminded that NSA has to report every dissemination, no matter how informal.

> This refers to information disseminated in a formal report as well as information disseminated informally such as written or oral collaboration with the FBI. We need to count every instance in which we take a piece of information derived from either of these two authorities and disseminate it outside of NSA.
>
> Normally an NSA product report is the record of a formal dissemination. In the context of the BR and PR/TT Programs, an official RFI response or Analyst Collaboration Record will also be viewed as dissemination. Because this FISC requirement goes beyond the more standard NSA procedures, additional diligence must be given to this requirement. NSA is required to report disseminations formal or informal to the FISC every 30 days.

I'm most interested in two other aspects of the training. First, it notes that not all queries obtained via the dragnet will be terrorism related.

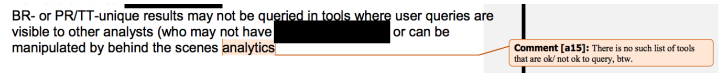
> It might seem as though the information would most certainly be counterterrorism-related since, due to the RAS approval process, you wouldn't

> have this U.S. person information from a query of BR or PR/TT if it weren't related to counterterrorism. In the majority of cases, it will be counterterrorism-related; however, the nature of the counterterrorism target is that it often overlaps with several other areas that include counternarcotics, counterintelligence, money laundering, document forging, people and weapons trafficking, and other topics that are not CT-centric. Thus, due to the fact that these authorities provide NSA access to a high volume of U.S. person information for counterterrorism purposes, the Court Order requires an explicit finding that the information is in fact related to counterterrorism prior to dissemination. Therefore, one of the approved decision makers must document the finding using the proper terminology. It must state that the information is related to counterterrorism and that it is necessary to understand the counterterrorism information.

Remember, this training was drafted in the wake of NSA's insistence that all these functional areas needed to be able to receive Internet dragnet data, which, of course, was just inviting the dissemination of information for reasons other than terrorism, especially given FISC's permission to use the dragnet to track Iranian "terrorism." Indeed, I still think think it overwhelmingly likely Shantia Hassanshahi got busted for proliferation charges using the phone dragnet (during a period when FISC was again not monitoring NSA very closely). And one of the things NSA felt the need to emphasize a year or so after NSA started being able to share this "counterterrorism" information outside of its counterterrorism unit was that they couldn't share information about money laundering or drug dealing or … counterproliferation unless there was a counterterrorism aspect to it. Almost as

if it had proven to be a problem.

The training program warns that results may not be put into queriable tools that untrained analysts have access to.



\

Note the absolutely hysterical review comment that said there's no list of which tools analysts couldn't use with 215 and PRTT dragnet results. Elsewhere, the training module instructs analysts to ask their manager, which from a process standpoint is a virtual guarantee there will be process violations.

This is interesting for two reasons. First, it suggests NSA was still getting in trouble running tools they hadn't cleared with FISC (the 215 IG Reports also make it clear they were querying the full database using more than just the contact-chaining they claim to have been limited to). Remember there were things like a correlations tool they had to shut down in 2009.

But it's also interesting given the approval, a year after this point, of an automatic alert system for use with the phone dragnet (which presumably was meant to replace the illegal alert system identified in 2009).

> In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to process its calling records.68 The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store."

> The ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within three "hops" of every currently approved selection term.69 Authorized analysts looking to conduct intelligence analysis may then use the records in the corporate store, instead of searching the full repository of records.70

That is, in 2011, NSA was moving towards such an automated system, which would constitute a kind of dissemination by itself. But it wasn't there yet *for the PATRIOT authorized collection.* Presumably it was for EO 12333 collection.

As it happened, NSA never did fulfill whatever requirements FISC imposed for using that automatic system with phone dragnet information, and they gave up trying in February 2014 when Obama decided to outsource the dragnet to the telecoms. But it would seem limits on the permission to use other fancy tools because they would amount to dissemination would likely limit the efficacy of these dragnets.

Clearly, in the weeks before NSA decided to shut down the PRTT dragnet, its lawyers were working hard to keep the agency in compliance with rules on dissemination. Then, they stopped trying and shut it down.

Both the replacement of PRTT with SPCMA and 702, and the replacement of the 215 dragnet with USAF, permit the government to disseminate metadata with far looser restrictions (and almost none, in the case of 702 and USAF metadata). It's highly likely this was one reason the NSA was willing to shut them down.

THE INTERNET DRAGNET WAS A CLUSTERFUCK … AND NSA DIDN'T CARE

Here's my best description from last year of the mind-boggling fact that NSA conducted 25 spot checks between 2004 and 2009 and then did a several months' long end-to-end review of the Internet dragnet in 2009 and found it to be in pretty good shape, only then to have someone discover that *every single record* received under the program had violated rules set in 2004.

> Exhibit A is a comprehensive end-to-end report that the NSA conducted in late summer or early fall of 2009, which focused on the work the agency did in metadata collection and analysis to try and identify people emailing terrorist suspects.
>
> The report described a number of violations that the NSA had cleaned up since the beginning of that year — including using automatic alerts that had not been authorized and giving the FBI and CIA direct access to a database of query results. It concluded the internet dragnet was in pretty good shape. "NSA has taken significant steps designed to eliminate the possibility of any future compliance issues," the last line of the report read, "and to ensure that mechanisms are in place to detect and respond quickly if any were to occur."
>
> But just weeks later, the Department of Justice informed the FISA Court, which oversees the NSA program, that the NSA had been collecting impermissible categories of data — potentially including content — for all five years of the program's existence.
>
> The Justice Department said the

> violation had been discovered by NSA's general counsel, which since a previous violation in 2004 had been required to do two spot checks of the data quarterly to make sure NSA had complied with FISC orders. But the general counsel had found the problem only after years of not finding it. The Justice Department later told the court that "virtually every" internet dragnet record "contains some metadata that was authorized for collection and some metadata that was not authorized for collection." In other words, in the more than 25 checks the NSA's general counsel should have done from 2004 to 2009, it never once found this unauthorized data.
>
> The following year, Judge John Bates, then head of FISC, emphasized that the NSA had missed the unauthorized data in its comprehensive report. He noted "the extraordinary fact that NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired." Bates went on, "[I]t must be added that those responsible for conducting oversight at NSA failed to do so effectively."

Even after these details became public in 2014 (or perhaps because the intelligence community buried such disclosures in documents with dates obscured), commentators have generally given the NSA the benefit of the doubt in its good faith to operate its dragnet(s) under the rules set by the FISA Court.

But an IG Report from 2007 (PDF 24-56) released in Charlie Savage's latest FOIA return should disabuse commentators of that opinion.

This is a report from early 2007, almost 3 years after the Stellar Wind Internet dragnet moved under FISA authority and close to 30 months after Judge Colleen Kollar-Kotelly ordered NSA

to implement more oversight measures, including those spot checks. We know that rough date because the IG Report post-dates the January 8, 2007 initiation of the FISC-spying compartment and it reflects 10 dragnet order periods of up to 90 days apiece (see page 21). So the investigation in it should date to no later than February 8, 2007, with the final report finished somewhat later. It was completed by Brian McAndrew, who served as Acting Inspector General from the time Joel Brenner left in 2006 until George Ellard started in 2007 (but who also got asked to sign at least one document he couldn't vouch for in 2002, again as Acting IG).

The IG Report is bizarre. It gives the NSA a passing grade on what it assessed.

> The management controls designed by the Agency to govern the collection, dissemination, and data security of electronic communications metadata and U.S. person information obtained under the Order are adequate and in several aspects exceed the terms of the Order.

I believe that by giving a passing grade, the IG made it less likely his results would have to get reported (for example, to the Intelligence Oversight Board, which still wasn't getting reporting on this program, and probably also to the Intelligence Committees, which didn't start getting most documentation on this stuff until late 2008) in any but a routine manner, if even that. But the report also admits it did not assess "the effectiveness of management controls[, which] will be addressed in a subsequent report." (The 2011 report examined here identified previous PRTT reports, including this one, and that subsequent report doesn't appear in any obvious form.) Then, having given the NSA a passing grade but deferring the most important part of the review, the IG notes "additional controls are needed."

And how.

As to the issue of the spot checks, mandated by the FISA Court and intended to prevent years of ongoing violations, the IG deems such checks "largely ineffective" because management hadn't adopted a methodology for those spot checks. They appear to have just swooped in and checked queries already approved by an analyst's supervisor, in what they called a superaudit.

Worse still, they didn't write anything down.

> As mandated by the Order, OGC periodically conducts random spot checks of the data collected [redaction] and monitors the audit log function. OGC does not, however document the data, scope, or results of the reviews. The purpose of the spot checks is to ensure that filters and other controls in place on the [redaction] are functioning as described by the Order and that only court authorized data is retained. [snip] Currently, an OGC attorney meets with the individuals responsible [redaction] and audit log functions, and reviews samples of the data to determine compliance with the Order. The attorney stated that she would formally document the reviews only if there were violations or other discrepancies of note. To date, OGC has found no violations or discrepancies.

So this IG review was done more than two years after Kollar-Kotelly had ordered these spot checks, during which period 18 spot checks should have been done. Yet at that point, NSA had *no documentary evidence a single spot check had been done*, just the say-so of the lawyer who claimed to have done them.

Keep in mind, too, that Oversight and Control were, at this point, implementing a new-and-improved spot-check process. That's what the IG reviewed, the new-and-improved process, because (of course) reviewers couldn't review the past process because there was no documentation of

it. It's the new-and-improved process that was inadequate to the task.

But that's not the only problem the IG found in 2007. For example, the logs used in auditing did not accurately document what seed had been used for queries, which means you couldn't review whether those queries really met the incredibly low bar of Reasonable Articulable Suspicion or that they were pre-approved. Nor did they document how many hops out analysts chained, which means any given query could have sucked in a great deal of Americans (which might happen by the third or fourth hop) and thrown them into the corporate store for far more intrusive anlaysis. While the IG didn't point this out directly, the management response made clear log files also didn't document whether a seed was a US person and therefore entitled to a First Amendment review. In short, NSA didn't capture any — any!!! — of the data that would have been necessary to assess minimal compliance with FISC orders.

NSA's lawyers also didn't have a solid list of everyone who had access to the databases (and therefore who needed to be trained or informed of changes to the FISC order). The Program Management Office had a list that it periodically compared to who was actually accessing the data (though as made clear later in the report, that included just the analysts). And NSA's Office of General Counsel would also periodically review to ensure those accessing the data had the information they needed to do so legally. But "the attorney conducting the review relie[d] on memory to verify the accuracy and completeness of the list." DOD in general is wonderfully neurotic about documenting any bit of training a given person has undergone, but with the people who had access to the Internet metadata documenting a great deal of Americans' communication in the country, NSA chose just to work from memory.

And this non-existent manner of tracking those with database access extended to auditing as

well. The IG reported that NSA also didn't track all queries made, such as those made by "those that have the ability to query the PRTT data but are not on the PMO list or who are not analysts." While the IG includes people who've been given new authorization to query the data in this discussion, it's also talking about techs who access the data. It notes, for example, "two systems administrators, who have the ability to query PRTT data, were also omitted from the audit report logs." The thing is, as part of the 2009 "reforms," NSA got approval to exempt techs from audits. I've written a lot about this but will return to it, as there is increasing evidence that the techs have always had the ability — and continue to have the ability — to bypass limits on the program.

There are actually far more problems reported in this short report, including details proving that — as I've pointed out before — NSA's training sucks.

But equally disturbing is the evidence that NSA really didn't give a fuck about the fact they'd left a database of a significant amount of Americans' communications metadata exposed to all sorts of control problems. The disinterest in fixing this problem dates back to 2004, when NSA first admitted to Kollar-Kotelly they were violating her orders. They did an IG report at the time (under the guidance of Joel Brenner), but it did "not make formal recommendations to management. Rather, the report summarize[d] key facts and evaluate[d] responsibility for the violation." That's unusual by itself: for audits to improve processes, they are supposed to provide recommendations and track whether those are implemented. Moreover, while the IG (who also claimed the clusterfuck in place in 2007 merited a passing grade) assessed that "management has taken steps to prevent recurrence of the violation," it also noted that NSA never really fixed the monitoring and change control process identified as problems back in

2004. In other words, it found that NSA hadn't fixed key problems IDed back in 2004.

As to this report? It did make recommendations and management even concurred with some of them, going so far as to agree to document (!!) their spot checks in the future. With others — such as the recommendation that shift supervisors should not be able to make their own RAS determinations — management didn't concur, they just said they'd monitor those queries more closely in the future. As to the report as a whole, here's what McAndrew had to say about management's response to the report showing the PRTT program was a clusterfuck of vulnerabilities: "Because of extenuating circumstances, management was unable to provide complete responses to the draft report."

So in 2007, NSA's IG demonstrated that the oversight over a program giving NSA access to the Internet metadata of a good chunk of all Americans was laughably inadequate.

And NSA's management didn't even bother to give the report a full response.

NSA TRIED TO ROLL OUT ITS AUTOMATED QUERY PROGRAM BETWEEN DEBATES ABOUT KILLING IT

As I noted earlier, after reporting in November that there was a debate in 2009 about ending the phone dragnet…

> To address their concerns, the former senior official and other NSA dissenters in 2009 came up with a plan that tracks

> closely with the Obama proposal that the Senate failed to pass on Tuesday. The officials wanted the NSA to stop collecting the records, and instead fashion a system for the agency to quickly send queries to the telephone companies as needed, letting the companies store the records as they are required to do under telecommunications rules.
>
> In a departure from the bill that failed Tuesday, however, they wanted to require the companies to provide the metadata in a standardized manner, to allow speedy processing and analysis in cases of an imminent terror plot. The lack of such a provision was among the reasons many Republicans and former intelligence officials said they opposed the 2014 legislation.
>
> By the end of 2009, Justice Department lawyers had concluded there was no way short of a change in law to make the program work while keeping the records in the hands of the companies, the former officials said.

The AP reported today that there was *also* a debate about ending the dragnet in 2013 (and if I'm not mistaken, the story has been updated to note that these were two separate debates)….

> The proposal to halt phone records collection that was circulating in 2013 was separate from a 2009 examination of the program by NSA, sparked by objections from a senior NSA official, reported in November by The Associated Press. In that case, a senior NSA code breaker learned about the program and concluded it was wrong for the agency to collect and store American records. The NSA enlisted the Justice Department in an examination of whether the search function could be preserved with the

> records stores by the phone companies.
>
> That would not work without a change in the law, the review concluded. Alexander, who retired in March 2014, opted to continue the program as is.
>
> But the internal debate continued, current and former officials say, and critics within the NSA pressed their case against the program. To them, the program had become an expensive insurance policy with an increasing number of loopholes, given the lack of mobile data. They also knew it would be deeply controversial if made public.
>
> By 2013, some NSA officials were ready to stop the bulk collection even though they knew they would lose the ability to search a database of U.S. calling records. As always, the FBI still would be able to obtain the phone records of suspects through a court order.

Between these two debates (indeed, between the time the NSA shut down the PATRIOT-authorized Internet dragnet and the second debate), on November 8, 2012, the NSA got FISC to approve an automated query.

> In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to process its calling records.68 The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store."

> The ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within three "hops" of every currently approved selection term.69 Authorized analysts looking to conduct intelligence analysis may then use the records in the corporate store, instead of searching the full repository of records.70

The January 3, 2014 dragnet order revealed that over the year-plus since FISC authorized this automated query, NSA still had not gotten it working.

> The Court understands that to date NSA has not implemented, and for the duration of this authorization will not as a technical matter be in a position to implement, the automated query process authorized by prior orders of this Court for analytical purposes. Accordingly, this amendment to the Primary Order authorizes the use of this automated query process for development and testing purposes only. No query results from such testing shall be made available for analytic purposes. Use of this automated query process for analytical purposes requires further order of this Court.

On March 27, 2014, Obama said he would move the dragnet to the telecoms.

The reauthorization signed the following day — dated March 28, 2014 — eliminated all approval for automated queries.

I suggested then — and given these stories, suspect may have been correct — that Obama agreed to move the dragnet to the telecoms because NSA never managed to do what they wanted to do (and probably, had done until 2009), automated queries, but they could achieve the

same desired result by moving production to the telecoms.

All proposed plans to move production to the telecoms shared several features, including the compelled assistance of the telecoms (like Section 702, in some ways), production of records in the form the government wanted, expansive immunity, and compensation. All also used "connection chaining" that didn't explicitly describe what made a (non-call or text) connection or how the telecom would establish such connections. I speculated last year that may have permitted the government to make use of the telecoms' access to geolocation in a way they couldn't do at NSA. I increasingly believe they also want telecoms to match all chaining through smart phones in what they've adopted as "connection chaining;" automated correlations, specifically, is something the government shut down in 2009 but which would be very productive if it could draw on everything the telecoms have.

None of that explains why the NSA wasn't able to ingest some cell phone production. But it may explain why NSA accepts moving the phone dragnet to the telecoms.

DEVIN NUNES THINKS CONGRESS NEEDS MORE CLASSIFIED BRIEFINGS TO UNDERSTAND PHONE DRAGNET

In an article describing the current state of play on the Section 215 sunset, WaPo quotes Devin Nunes claiming that the poor maligned phone dragnet is just misunderstood. So

he plans on having more briefings (curiously, just for the Republican caucus).

> "NSA programs, including the bulk telephone metadata program, are crucial anti-terror and foreign intelligence tools that should be reauthorized," said Rep. Devin Nunes (R-Calif.), chairman of the House Intelligence Committee.
>
> He told reporters on Tuesday that he felt the program has been misunderstood and that he would hold classified briefings for the GOP caucus.

I don't mean to mock Nunes. After all, I've been saying for well over a year that the public assessments of the phone dragnet don't actually measure how the government really uses it (below the rule I've copied the part of this post that describes other ways we know they use it). And that was before the phone dragnet orders replaced "contact chaining" with "connection chaining" over a year ago, which presumably adds a correlating function to the mix (that is, the government also uses the phone dragnet to identify a person's multiple phone-based identities, potentially including smart phone identities).

But I do think it worth noting two things.

First, Nunes' decision to tell Republicans more, coming relatively soon after he took over the House Intelligence Chair from Mike Rogers, suggests that Mike Rogers was never fully forthcoming — not even in the secret briefings he gave in lieu of passing on Executive Branch explanations of the phone dragnet — about what it did.

But Nunes' response is *not* to require the government to itself explain publicly what it's really doing with the phone dragnet. But instead to hold classified briefings that often serve as a means to buy silence from those who attend.

In any case, that story you've been told for almost two years about how the phone dragnet identifies who is two degrees away from Osama bin Laden? Unsurprisingly, it's nowhere near the full story.

[A]ssessments of the phone dragnet […] don't even take the IC at its word in its other, quieter admissions of how it uses the dragnet (notably, in none of Stone's five posts on the dragnet does he mention any of these — one, two, three, four,five — raising questions whether he ever learned or considered them). These uses include:

- Corporate store
- "Data integrity" analysis
- Informants
- Index

Corporate store: As the minimization procedures and a few FISC documents make clear, once the NSA has run a query, the results of that query are placed in a "corporate store," a database of all previous query results.

ACLU's Patrick Toomey has described this in depth, but the key takeaways are once data gets into the corporate store, NSA can use "the full range of SIGINT analytic tradecraft" on it, and none of that activity is audited.

NSA would have you believe very few Americans' data gets into that corporate store, but even if the NSA treats queries it says it does, it could well be in the millions. Worse, if NSA doesn't do what they say they do in removing high volume numbers like telemarketers, pizza joints, and cell voice mail numbers, literally everyone could be in the corporate store. As far as I've

seen, the metrics measuring the phone dragnet only involve tips going out to FBI and not the gross number of Americans' data going into the corporate store and therefore subject to "the full range of analytic tradecraft," so we (and probably even the FISC) don't know how many Americans get sucked into it. Worse, we don't know what's included in "the full range of SIGINT analytic tradecraft" (see this post for some of what they do with Internet metadata), but we should assume it includes the data mining the government says it's not doing on the database itself.

The government doesn't datamine phone records in the main dragnet database, but they're legally permitted to datamine anyone's phone records who has come within 3 degrees of separation from someone suspected of having ties to terrorism.

"Data integrity" analysis: As noted, the NSA claims that before analysts start doing more formal queries of the phone dragnet data, "data integrity" analysts standardize it and do something (it's unclear whether they delete or just suppress) "high volume numbers." They also — and the details on this are even sketchier — use this live data to develop algorithms. This has the possibility of significantly changing the dragnet and what it does; at the very least, it risks eliminating precisely the numbers that might be most valuable (as in the Boston Marathon case, where a pizza joint plays a central role in the Tsarnaev brothers' activities). The auditing on this activity has varied over time, but Dianne Feinstein's bill would eliminate it by statute. Without such oversight, data integrity analysts have in the past, moved chunks of data, disaggregated them from any identifying (collection date and source) information, and done … we don't know what with it. So one question about the data integrity analyst position is how narrowly scoped the high volume numbers are (if it's not narrow, then everyone's in the corporate store); an even bigger is what they do with the data in often unaudited behavior before it's place into

the main database.

Informants: Then there's the very specific, admitted use of the dragnet that no one besides me (as far as I know) has spoken about: to find potential informants. From thevery start of the FISC-approved program, the government maintained the dragnet "may help to discover individuals willing to become FBI assets," and given that the government repeated that claim 3 years later, it does seem to have been used to find informants.

This is an example of a use that would support "connecting the dots" (as the program's defenders all claim it does) but that could ruin the lives of people who have no tie to actual terrorists (aside from speaking on the phone to someone one or two degrees away from a suspected terror affiliate). The government has in the past told FISCR it might use FISA data to find evidence of other crimes — even rape — to coerce people to become informants, and in some cases, metadata (especially that in the corporate store, enhanced by "the full range of analytic tradecraft") could pinpoint not just potential criminals, but people whose visa violations and extramarital affairs might make them amenable to narcing on the people in their mosque (with the additional side effect of building distrust within a worship community). There's not all that much oversight over FBI's use of informants in any case (aside from permitting us to learn that they're letting their informants commit more and more crimes), so it's pretty safe to assume no one is tracking the efficacy of the informants recruited using the powerful tools of the phone dragnet.

Index: Finally, there's the NSA's use of this metadata as a Dewey Decimal System (to useJames Clapper's description) to pull already-collected content off the shelf to listen to — a use even alluded to in the NSA's declarations in suits trying to shut down the dragnet.

> Section 215 bulk telephony metadata complements other counterterrorist-

> related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

Don't get me wrong. Given how poorly the NSA has addressed its longterm failure to hire enough translators in target languages, I can understand how much easier it must be to pick what to read based on metadata analysis (though see my concerns, above, about whether the NSA's assessment techniques are valid). But when the NSA says, "non-US persons" here, what they mean is "content collected by targeting non-US persons," which includes a great deal of content of US persons.

Which is another way of saying the dragnet serves as an excuse to read US person content.

UNIT 8200 REFUSENIKS MAKE VISIBLE FOR ISRAEL WHAT REMAINS INVISIBLE IN THE US

Last week, 43 reserve members of Israel's equivalent to the NSA, Unit 8200, released a letter announcing they would refuse to take actions against Palestinians because the spying done on them amounts to persecution of innocent people. The IDF has responded the same way government agencies here would — scolding the whistleblowers for not raising concerns in official channels. But the letter has elicited rare public discussion about the ethics and morality of spying.

One of the allegations made by the refuseniks highlighted in the English press is that Israel used SIGINT to recruit collaborators, which in turn divides the Palestinian community.

> The Palestinian population under military rule is completely exposed to espionage and surveillance by Israeli intelligence. While there are severe limitations on the surveillance of Israeli citizens, the Palestinians are not afforded this protection. There's no distinction between Palestinians who are, and are not, involved in violence. Information that is collected and stored harms innocent people. *It is used for political persecution and to create divisions within Palestinian society by recruiting collaborators and driving parts of Palestinian society against itself.* In many cases, intelligence prevents defendants from receiving a fair trial in military courts, as the evidence against them is not revealed. Intelligence allows for the continued control over millions of people through thorough and intrusive supervision and

> invasion of most areas of life. This does not allow for people to lead normal lives, and fuels more violence further distancing us from the end of the conflict. [my emphasis]

These refuseniks, apparently, have access both to the intelligence they collect and how it is used. That means they're in a position to talk about the effects of Unit 8200's spying. And press coverage has made it sound like something that would uniquely happen to occupied Palestinians.

It's not.

We know of one way that the NSA's dragnet is definitely being used to recruit informants (aka collaborators), and another whether it it permissible to use.

The first way is via the phone dragnet. As I have noted, the government has twice told the FISA Court — once in 2006 and once in 2009 — that FBI uses dragnet derived information to identify people who might cooperate (aka inform or collaborate) in investigations. Once people come up on a 2-degree search, they are dumped into the corporate store indefinitely, data mined with sufficient information to find embarrassing and illegal things. Apparently, FBI uses such data to coerce cooperation, though we have no details on the process.

All the revealing things metadata shows? The government uses that information to obtain informants.

One way the government probably does this is by using the connections identified by metadata analysis (remember, this is not just phone and Internet data, but also includes financial and travel data, at a minimum) to put people on the No Fly list, regardless of whether they are a real threat to this country. Then, No Fly listees have alleged, FBI promises help getting them off that life-altering status if they inform on their community.

More troubling still is FBI's uncounted use of warrantless back door searches of US person content when conducting assessments. As I noted, in addition to doing assessments in response to "tips," the FBI will use them to profile communities or identify potential informants.

> As the **FBI's Domestic Investigations and Operations Guide** describes, assessments are used for "prompt and extremely limited checking out of initial leads." No factual predicate (that is, no real evidence of wrong-doing) is required before the FBI starts an assessment. While FBI cannot use First Amendment activities as the sole reason for assessments, they can be considered. In addition to looking into leads about individual people, FBI uses assessments as part of the process for Domain Assessments (what **FBI calls their profiling of Muslim communities**) and the selection of informants to try to recruit. In some cases, an Agent doesn't need prior approval to open an assessment; in others, they may get oral approval (though for several kinds, an Agent must get a formal memo approved before opening an assessment). And while Agents are supposed to record all assessments, for some assessments, they're very cursory reports — basically complaint forms. That is, for certain types of assessments, FBI is not generating its most formal paperwork to track the process.

So while I can't point to a DOJ claim to FISC that these back door searches are useful because they help find informants, it appears to be possible. Plus, as early as 2002, Ted Olson said they would use evidence of rape collected using traditional FISA to talk someone into cooperating (aka inform or collaborate); that was the reason he gave for blowing the wall between intelligence and criminal investigations

to smithereens.

Indeed, knowing the way the government uses phone dragnet information as an index to collected content, the government may well use phone dragnet metadata to pick which Americans to subject to warrantless back door searches.

It sounds really awful when we hear about Israel using SIGINT — including information we provide without minimizing it — to spy on Palestinians.

But we have a good deal of reason to believe the US intelligence community — in collaboration — does similar things, spying on Muslim communities and using SIGINT to recruit collaborators that end up sowing paranoia and distrust in the communities.

Not only don't we have a group of refuseniks who, among themselves, can explain how all of this works. But how the FBI uses all this data is precisely what the government intends to keep secret under the so-called "transparency" provisions of USA Freedom Act. While I will provide more detail in a follow-up post, remember that the FBI refuses to count its back door searches, which means it would be almost impossible for anyone to get a real sense of how these warrantless back door searches on US persons are used. It also has asserted it does not need to disclose evidence derived from Section 215 to criminal defendants, which is another way the evidence against defendants gets hidden.

It's awful that Israel is doing it. But it's even worse that we're almost certainly doing the same, but that we can only find hints of how it is being done.

JAMES CLAPPER'S LETTER DIDN'T ENDORSE S 2685; IT ENDORSED HR 3361

I'm sorry to return to James Clapper's letter that has been grossly misreported as endorsing Patrick Leahy's USA Freedom Act.

In this post I pointed out what Clapper's letter really said. In this one, I described why it is so inexcusable that Clapper emphasized FBI's exemption from reporting requirements (I will have a follow-up soon about why that earlier post just scratches the surface). And this post lays out some — but not all — the ways Clapper's letter said he would gut the Advocate provision.

But I think there's a far better way of understanding Clapper's letter. He didn't endorse Leahy's USAF, S 2685. He endorsed USA Freedumber, HR 3361.

Below the rule I've put a summary of changes from USA Freedumber to Leahy USA Freedom, HR 3361 to S 2685. I did it a very long time ago, and there are things I'd emphasize differently now, but it will have to do for now (it may also be helpful to review this summary of how USA Freedumber made USA Freedumb worse). Basically, S 2685 improved on HR 3361 by,

- Tightening the definition of "specific selection term"
- Adding transparency (though, with exemptions for FBI reporting)
- Improving the advocate
- Limiting prospective CDR collection (but not retention and therefore probably dissemination) to

This closely matches what the coalition that signed onto S 2685 laid out as the improvements from HR 3361 to S 2685.

> [T]he new version of the bill:
>
> - *Strengthens and clarifies the ban on "bulk" collection of records, including by tightening definitions to ensure that the government can't collect records for everyone in a particular geographic area or using a particular communication service, and by adding new post-collection minimization procedures;*
> - *Allows much more detailed transparency reporting by companies—and requires much more detailed transparency reporting by the government—about the NSA's surveillance activities; and*
> - *Provides stronger reforms to the secret Foreign Intelligence Surveillance Court's processes, by creating new Special Advocates*

> *whose duty is to advocate to the court in favor of privacy and civil liberties, and by strengthening requirements that the government release redacted copies or summaries of the court's significant decisions.*

Though as I explained here, there is no public evidence the minimization procedures required by the bill are even as stringent as what the FISC currently imposes on most orders, so the minimization procedures of S 2685 might — like the emergency procedures do — actually weaken the status quo.

Here are three of the key passages from Clapper's letter that I believe would address the intent of the bill as written.

- "Recognizing that the terms [laid out in the definition of specific selection term] enumerated in the statute may not always meet operational needs, the bill permits the use of other terms."
- "The transparency provisions in this bill … recognize the technical limitations on our ability to report certain types of information."
- "The appointment of an amicus in selected cases, as

> appropriate, need not interfere with important aspects of the FISA process, including the process of ex parte consultation between the Court and the government. We are also aware of the concerns that the Administrative Office of the U.S. Courts expressed in a recent letter, and we look forward to working with you and your colleagues to address those concerns."

In other words, the limiting language in Clapper's letter very clearly maps the changes from HR 3361 to S 2685.

He clearly says he doesn't have to follow the new limits on specific selection terms. He signals he will use his authority to make classification and privilege determinations to keep information away from the amicus (or retain ex parte procedures via some other means). And by endorsing John Bates' letter, he revealed his intention to take out requirements that the amicus advocate in favor of privacy and civil liberties. In addition — this is the part of Bates' letter I missed in my previous analysis — he thereby endorsed Bates' recommendation to "delet[e] this provision [specifying that the Court must release at least a summary], leaving in place the provision that significant FISA court decision would continue to be released, whenever feasible, in redacted form."

Plus, as I mentioned, his use of "metadata" rather than "Call Detail Record" suggests he may play with that laudable limit in the bill as well.

I think Clapper's read on the exemption for FBI is totally a fair reading of the bill; I just

happen to think the Senate is doing a great deal of affirmative damage by accepting it. (Again, I hope to explain more why that is the case in the next day or so.)

Voila! Clapper's "endorsement" of the bill managed to carve out almost all the improvements from HR 3361 to S 2685 (as well as emphasize Congress' ratification for the FBI exemption, the huge reservation on the one improvement he left untouched). The only other improvement Clapper left in place was the limit on collection of prospective phone record to counterterrorism purposes.

That's it. If Clapper's views hold sway, that's all this bill is: USA Freedumber with the retention of the status quo counterterrorism application for CDR collection.

My views:

Bulk

This gets closer to banning bulk collection than USA Feedumber, but language about IP addresses and distinctions between persons and individuals still concerns me

Transparency

Much of the transparency is good and welcome, but note this excludes FBI from back door search reporting, which is actually quite alarming.

Advocate

The FISA Advocate is better, though still doesn't prevent the government from stymying it (for example through "need to know" language). I'm also not convinced PCLOB will be a good faith entity long term, particularly if we lose the Senate (Certainly Cook and Brand are not civil libertarians; they're defenders of these programs, which is what we should expect if GOP gets another appointee). Also, I think the FISCR fast-track review could backfire in significant

ways, because it could preclude real adversarial review if anyone ever gets standing.

NSLs

I'm not convinced the NSL language fixes the Doe problems—it would seem to just provide the government another way to gag these things, but I'd have to look closer to be sure.

CDR program

This doesn't change that the CDR chaining is on connections, not calls. I think this is a very dangerous provision given that no one I've talked to outside of Intel Committees knows what it means (and we should assume it means, at a minimum, location chaining). Assuming this will get delayed beyond recess, it seems like a good point to demand answers on. And if those come back reasonably it might be wise to add interpretations of "connections" to the transparency requirements?

Also, while the limitation on CDR chaining to CT purposes is good, the bill still permits retention for any FI purpose, which we know thanks to PCLOB means they'll retain everything. I think it very likely that under this program more Americans will be stuck in the corporate store indefinitely than they are under the current program, and by tying retention to FI, I suspect it will weaken minimization protections on dissemination of that data, too.

Note that the bill still permits CDR collection under b2B. What's to prevent them from continuing to do bulk collection there?

Finally, I continue to believe the Rule of Construction on content is meaningless; given what Zoe Lofgren has gotten James Cole to agree to, we should assume FISC has already authorized content (especially URL searches) collection. So the government already has the authority.

PRTT

I still don't see why inventing new privacy protections, rather than codifying minimization

procedures approved by the court, makes any sense. And the Rule of Construction not changing FISC's current authority is meaningless, as it has no legal authority, it has just assumed authority.

Here are further comments organized by page number.

(6) Retains the chaining on "connections." Thus far I have met no one who knows what this means outside of the intelligence committees, and language addressing it in phone dragnet orders remains redacted. Particularly given that every government witness has only admitted to call chaining, not connection chaining, there seems to be a need to discuss what connection chaining is, particularly given that once the government gets inside a smart phone at a telecom they might be able to use things like calendars and phone books to make such connections. The requirement that the product at each step be a CDR limits this somewhat, but it doesn't limit it all that much. This will likely result in a might higher hit rate than what is currently supposed to go on in chaining using 215 data.

(7) The bill retains the meaningless destruction requirement from USA Freedumber, tied to FI purpose rather than CT purpose (which is what the current dragnet is supposed to have). Particularly given confirmation from both PCLOB and WaPo in the interim that destruction requirements tied to FI mean nothing gets destroyed, this is a problem. It will mean everything will be retained—and we still don't know whether this includes pizza joint connections or not.

(16) I've heard people express significant concerns about IP addresses, which can be quite broad. So this definition of address may actually include some flux in it. It certainly could include a whole company, depending on what they do with their web service.

(17) Specific selection term: This is generally better than what we had. There are three questions I have. First, why use people in 3Ai (which applies to b2B collection and other authorities like PRTT and NSL) and individual in 3B, which applies to b2C collection? With the additional minimization procedures, they basically admit the primary definition of SST needs additional minimization should raise questions. I know this is meant to serve for the collection of things like TATP precursors (they used 215 to get acetone and hydrogen peroxide in 2009). Doesn't that mean something is still very broad?

(27) In my opinion the rule of construction on minimization procedures is meaningless. By law, FISA has no authority under pen registers authority to impose minimization procedures; it's just that they did in order to approve the broad requests made. What is the explanation for providing this authority to the AG? In other words, privacy procedures are not "new," they're just done now with the involvement of the FISC. Why change that in law?

Also, FBI has (or did in 2012, after the NSA PRTT program was shut down) a PRTT bulk program. If Senators don't know what that is, it would seem time to answer those questions in the context of this discussion.

(30) Note, the Special Advocates are now required to be attorneys and weren't under USA Freedumber. There may be a good reason for this, but it would seem to rule out the kind of technical people who may be just as necessary to this process. With the ability to request a technical advisor that may not be a problem but it is worth noting.

(33) The language on classified information seems to build in a presumption that the executive will determine access. Given how the government has used "need to know" designation to prevent lawyers from accessing information they need, that may be a problem.

(35) The FISCR review actually seems very dangerous as written. First, because the FISC staffers will be the ones staffing the FISCR judges; they don't have independent staffers. So they will effectively be a continuity of view, not a new one. Moreover, this system will present an adversary-less system of giving decisions appellate sanction in secret. Even in the two known cases, In Re Sealed 2002 and Yahoo, there was some kind of adversary or amicus. It's not clear this would be as robust (particularly given that the FISC only may, not shall, appoint an amicus). In other words, while the intent here may be laudable, in practice it might fast track appellate sanction for broad expansions of law without 1) real adversarial proceedings or 2) notice to the public. At the very least, this provision should require that Congress get full notification before something gets appealed, otherwise this could all happen in secret before Congress gets their required notice.

(40) Note the FCRA NSL specifically uses customer or account and SST. Why isn't this available elsewhere?

(75) Why does the back door search on content count "search terms that included information concerning a United States person that were used to query any database of the contents" but the search on metadata counts "queries initiated by an officer, employee, or agent of the United States whose search terms included information concerning a United States person in any database of noncontents"?

(79) The transparency exempts FBI from the most important requirements (covering 702 back door searches and 215 searches of both the traditional fashion and the new CDR program).

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

> of Investigation.

This seems crazy. It is not just a transparency problem, but a management problem, that FBI refuses to count these numbers. Not only would it provide a badly misrepresentative number, but wouldn't make FBI impose the kind of management oversight they need on precisely the kind of back door searches most likely to land someone in prison.

(80) After having seen the WaPo do a statistical sample, this bill permits DNI to claim they can't do a sample.That seems overly generous.

(83) The description of someone who is "a party" to an electronic communication may not count those who get collected in chat rooms as lurkers, or similar such things. Does someone using a tracked URL get tracked here, for example?