FINGERPRINTS AND THE PHONE DRAGNET'S SECRET "CORRELATIONS" ORDER

Yesterday, I noted that ODNI is withholding a supplemental opinion approved on August 20, 2008 that almost certainly approved the tracking of "correlations" among the phone dragnet (though this surely extends to the Internet dragnet as well).

I pointed out that documents released by Edward Snowden suggest the use of correlations extends well beyond the search for "burner" phones.

At almost precisely the same time, Snowden was testifying to the EU. The first question he answered served to clarify what "fingerprints" are and how XKeyscore uses them to track a range of innocent activities. (This starts after 11:16, transcription mine.)

> It has been reported that the NSA's XKeyscore for interacting with the raw signals intercepted by mass surveillance programs allow for the creation of something that is called "fingerprints."
>
> I'd like to explain what that really means. The answer will be somewhat technical for a parliamentary setting, but these fingerprints can be used to construct **a kind of unique signature** for any individual or group's communications which are often **comprised of a collection of "selectors" such as email addresses, phone numbers, or user names**.
>
> This allows State Security Bureaus to instantly identify the movements and activities of you, your computers, or other devices, your personal Internet

> accounts, or even key words or other uncommon strings that indicate an individual or group, out of all the communications they intercept in the world are associated with that particular communication. Much like a fingerprint that you would leave on a handle of your door or your steering wheel for your car and so on.
>
> However, though that has been reported, that is the smallest part of the NSA's fingerprinting capability. You must first understand that any kind of Internet traffic that passes before these mass surveillance sensors can be analyzed in a protocol agnostic manner – metadata and content, both. And it can be today, right now, searched not only with very little effort, via a complex regular expression, which is a type of shorthand programming. But also via any algorithm an analyst can implement in popular high level programming languages. Now, this is very common for technicians. It not a significant work load, it's quite easy.
>
> This provides a capability for analysts to do things like associate unique identifiers assigned to untargeted individuals via unencrypted commercial advertising networks through cookies or other trackers – common tracking means used by businesses everyday on the Internet – with personal details, such as individuals' precise identity, personal identity, their geographic location, their political affiliations, their place of work, their computer operating system and other technical details, their sexual orientation, their personal interests, and so on and so forth. There are very few practical limitations to the kind of analysis that can be technically performed in this manner, short of the actual imagination

> of the analysts themselves.
>
> And this kind of complex analysis is in fact performed today using these systems. I can say, with authority, that the US government's claim that "keyword filters," searches, or "about" analysis, had not been performed by its intelligence agencies are, in fact, false. I know this because I have personally executed such searches with the explicit authorization of US government officials. And I can personally attest that these kind of searches may scrutinize communications of both American and European Union citizens without involvement of any judicial warrants or other prior legal review.
>
> What this means in non-technical terms, more generally, is that I, an analyst working at NSA, or, more concerningly, an analyst working for a more authoritarian government elsewhere, can without the issue of any warrant, create an algorithm that for any given time period, with or without human involvement, sets aside the communications of not only targeted individuals, but even a class of individual, and that just indications of an activity – or even just indications of an activity that I as the analyst don't approve of – something that I consider to be nefarious, or to indicate nefarious thoughts, or pre-criminal activity, even if there's no evidence or indication that's in fact what's happening. that it's not innocent behavior. The nature of the mass surveillance – of these mass surveillance technologies – create a de facto policy of assigning guilt by association rather than on the basis of specific investigations based on reasonable suspicion.

> Specifically, mass surveillance systems like XKeyscore provide organizations such as the NSA with the technical ability to trivially track entire populations of individuals who share any trait that is discoverable from unencrypted communications. For example, these include religious beliefs, political affiliations, sexual orientations, contact with a disfavored individual or group, history of donating to specific or general causes, interactions of transactions with certain private businesses, or even private gun ownership. It is a trivial task, for example, to generate lists of home addresses for people matching the target criteria. Or to collect their phone numbers, to discover their friends, or even, to analyze the proximity and location of their social connections by automating the detection of factors such as who they share pictures of their children with, which is capable of machine analysis.
>
> I would hope that this goes without saying, but let me be clear that the NSA is not engaged in any sort of nightmare scenarios, such as actively compiling lists of homosexual individuals to round them up and send them into camps, or anything of that sort. However, they still deeply implicate our human rights. We have to recognize that the infrastructure for such activities has been built, and is within reach of not just the United States and its allies, but of any country today. And that includes even private organizations that are not associated with governments.
>
> Accordingly, we have an obligation to develop international standards, to protect against the routine and substantial abuse of this technology, abuses that are ongoing today. I urge

> the committee in the strongest terms to bear in mind that this is not just a problem for the United States, or the European Union, but that this is in fact a global problem, not an isolated issue of Europe versus the Five Eyes or any other [unclear]. These technical capabilities don't merely exist, they're already in place and actively being used without the issue of any judicial warrant. I state that these capabilities are not yet being used to create lists of all the Christians in Egypt, but let's talk about what they are used for, at least in a general sense, based on actual real world cases that I can assert are in fact true.
>
> Fingerprints — for example, the kind used of XKeyscore — have been used — I have specific knowledge that they have been used — to track and intercept, to track, intercept, and monitor the travels of innocent citizens, who are not suspected of anything worse than booking a flight. This was done, in Europe, against EU citizens but it is of course not limited to that geographic region, nor that population. Fingerprints have also been used to monitor untold masses of people whose communications transit the entire country of Switzerland over specific routes. They're used to identify people — Fingerprints are used to identify people who have had the bad luck to follow the wrong link on an Internet site, on an Internet forum, or even to download the wrong file. They've been used to identify people who simply visit an Internet sex forum. They've also been used to monitor French citizens who have never done anything wrong other than logging into a network that's suspected of activity that's associated with a behavior that the National Security Agency does not approve of.

> This mass surveillance network, constructed by the NSA, which, as I pointed out, is an Agency of the US military Department of Defense, not a civilian agency, and is also enabled by agreements with countries such as the United Kingdom, Australia, and even Germany, is not restricted for being used strictly for national security purposes, for the prevention of terrorism, or even for foreign intelligence more broadly.
>
> XKeyscore is today secretly being used for law enforcement purposes, for the detection of even non-violent offenses, and yet this practice has never been declared to any defendant or to any open court.
>
> We need to be clear with our language. These practices are abusive. This is clearly a disproportionate use of an extraordinarily invasive authority, an extraordinarily invasive means of investigation, taken against entire populations, rather than the traditional investigative standard of using the least intrusive means or investigating specifically named targets, individuals, or groups. The screening of trillions — I mean that literally, trillions — of private communications for the vaguest indications of associations or some other nebulous pre-criminal activity is a violation of the human right to be free from unwarranted interference, to be secure in our communications and our private affairs, and it must be addressed. These activities — routine, I point out, unexceptional activities that happen every day — are only a tiny portion of what the Five Eyes are secretly doing behind closed doors, without the review, consent, or approval of any public body. This technology represents the most significant — what I

> consider the most significant.new threat to civil rights in modern times.

Now, this doesn't guarantee that the NSA correlates identifiers to dump them into XKeyscore (which is, as far as I know, used only on data collected outside the US; the "about" 702 collection is a more limited version of what is done in the US, with returned data likely dumped into databases used with XKeyscore). But Snowden makes it clear such fingerprints involve precisely the identifiers, including phone numbers, used in the domestic dragnets.

Moreover, we know that data in the corporate store — all those people who are two or three degrees away from someone who has been digitally stop-and-frisked — is subject to all the analytical authorities the NSA uses, which clearly includes fingerprinting and use in XKeyscore.

"Correlations" — as the NSA uses in language with the FISC and Congress — are almost certainly either fingerprints, or subset of the fingerprinting process.

And this is, almost certainly, what the government is hiding in that August 20, 2008 order.

THE AUGUST 20, 2008 CORRELATIONS OPINION

On August 18, 2008, the government described to the FISA

Court how it used a particular tool to establish correlations between identifiers. (see page 12)

> A description of how [name of correlations tool] is used to correlate [description of scope of metadata included] was included in the government's 18 August 2008 filing to the FISA Court,

On August 20, 2008, the FISC issued a supplemental opinion approving the use of "a specific intelligence method in the conduct of queries (term "searches") of telephony metadata or call detail records obtained pursuant to the FISC's orders under the BR FISA program." The government claims that it cannot release any part of that August 20, 2008 opinion, which given the timing (which closely tracks with the timing of other submissions and approvals before the FISC) and the reference to both telephony metadata and call detail records almost certainly approves the use of the dragnet – and probably not just the phone dragnet – to establish correlations between a target's multiple communications identifiers.

As ODNI's Jennifer Hudson described in a declaration in the EFF suit, the government maintains that it cannot release this opinion, in spite of (or likely because of) ample description of the correlations function elsewhere in declassified documents.

> The opinion is only six pages in length and the specific intelligence method is discussed at great length in every paragraph of this opinion, including the title. Upon review of this opinion, I have determined that there is no meaningful, segregable, non-exempt information that can be released to the plaintiff as the entire opinion focuses on this intelligence method. Even if the name of the intelligence method was redacted, the method itself could be deduced, given other information that the DNI has declassified pursuant to the President's transparency initiative and the sophistication of our Nation's adversaries **[Ed: did she just call me an "adversary"?!?]** and foreign intelligence services.
>
> [snip]
>
> The intelligence method is used to conduct queries of the bulk metadata, and if NSA were no longer able to use this method because it had been compromised, NSA's ability to analyze bulk metadata would itself be compromised. A lost or reduced ability to detect communications chains that link to identifiers associated with known and suspected terrorist operatives, which can lead to the identification of previously unknown persons of interest in support of anti-terrorism efforts both within the United States and abroad, would greatly impact the effectiveness of this program as there is no way to know in advance which numbers will be responsive to the authorized queries.

ACLU's snazzy new searchable database shows that this correlations function was discussed in at least three of the officially released documents thus far: in the June 25, 2009 End-to-End Review, in a June 29, 2009 Notice to the House

Intelligence Committee, and in the August 19, 2009 filing submitting the End-to-End Review to the FISC.

In addition to making it clear this practice was explained to the FISC just before the Supplemental Opinion in question, these documents also describe a bit about the practice.

They define what a correlated address is (and note, this passage, as well as other passages, do not limit correlations to telephone metadata — indeed, the use of "address" suggests correlations include Internet identifiers).

> The analysis of SIGINT relies on many techniques to more fully understand the data. One technique commonly used is correlated selectors. A communications address, or selector, is considered correlated with other communications addresses when each additional address is shown to identify the same communicant as the original address.

They describe how the NSA establishes correlations via many means, but primarily through one particular database.

> NSA obtained [redacted] correlations from a variety of sources to include Intelligence Community reporting, but the tool that the analysts authorized to query the BR FISA metadata primarily used to make correlations is called [redacted].
>
> [redacted] — a database that holds correlations [redacted] between identifiers of interest, to include results from [redacted] was the primary means by which [redacted] correlated identifiers were used to query the BR FISA metadata.

They make clear that NSA treated all correlated

identifiers as RAS approved so long as one identifier from that user was RAS approved.

> In other words, if there: was a successful RAS determination made on any one of the selectors in the correlation, all were considered .AS-a. ,)roved for purposes of the query because they were all associated with the same [redacted] account

And they reveal that until February 6, 2009, this tool provided "automated correlation results to BR FISA-authorized analysts." While the practice was shut down in February 2009, the filings make clear NSA intended to get the automated correlation functions working again, and Hudson's declaration protecting an ongoing intelligence method (assuming the August 20, 2008 opinion does treat correlations) suggests they have subsequently done so.

When this language about correlations first got released, it seemed it extended only so far as the practice — also used in AT&T's Hemisphere program — of matching call circles and patterns across phones to identify new "burner" phones adopted by the same user. That is, it seemed to be limited to a known law enforcement approach to deal with the ability to switch phones quickly.

But both discussions of the things included among dragnet identifiers — including calling card numbers, handset and SIM card IDs — as well as slides released in stories on NSA and GCHQ's hacking operations (see above) make it clear NSA maps correlations very broadly, including multiple online platforms and cookies. Remember, too, that NSA analysts access contact chaining for both phone and Internet metadata from the same interface, suggesting they may be able to contact chain across content type. Indeed, NSA presentations describe how the advent of smart phones completely breaks down the distinction between phone and Internet metadata.

In addition to mapping contact chains and identifying traffic patterns NSA can hack, this correlations process almost certainly serves as the glue in the dossiers of people NSA creates of individual targets (this likely only happens via contact-chaining after query records are dumped into the corporate store).

Now it's unclear how much of this Internet correlation the phone dragnet immediately taps into. And my assertion that the August 20, 2008 opinion approved the use of correlations is based solely on … temporal correlation. Yet it seems that ODNI's unwillingness to release this opinion serves to hide a scope not revealed in the discussions of correlations already released.

Which is sort or ridiculous, because far more detail on correlations have been released elsewhere.

INITIAL THOUGHTS ON OBAMA'S DRAGNET FIX

The White House has rolled out the bare sketch of its proposal to fix the dragnet. The sketch says,

- the government will not collect these telephone records in bulk; rather, the records would remain at the telephone companies for the length of time they currently do today;
- absent an emergency situation, the government would obtain the records

only pursuant to individual orders from the FISC approving the use of specific numbers for such queries, if a judge agrees based on national security concerns;

- the records provided to the government in response to queries would only be within two hops of the selection term being used, and the government's handling of any records it acquires will be governed by minimization procedures approved by the FISC;
- the court-approved numbers could be used to query the data over a limited period of time without returning to the FISC for approval, and the production of records would be ongoing and prospective; and
- the companies would be compelled by court order to provide technical assistance to ensure that the records can be queried and that results are transmitted to the government in a usable format and in a timely manner.

The most important question asked in a conference call on this is what the standard for querying would be. Congress would decide that,

but it Reasonable Articulable Suspicion would be the starting point.

That sketch doesn't really answer a lot of questions about the program, including:

- Will this program be used for "national security concerns" beyond counterterrorism? Never once did the conference call say it was limited to CT, and several comments suggested it could be used more broadly.
- What kind of protections will the data (the overwhelming number of which would be innocent people) get once it lands at NSA (see the minimization procedures noted above)? Will it resemble the corporate store of forever datamining that currently exists?
- Who will do the data integrity that currently requires access to the raw data, which has a dramatic influence on how much data would be responsive to a 2-hop query? The required "technical assistance" might include some of it (it definitely includes formatting the data such that NSA can legally accept

it, which has caused a problem with cell data). But does Verizon or NSA or Booz go through the raw data and pull out the high volume numbers?

- For how long will these orders be granted? (It sounds like the White House will use this to entice congressional support.)
- Will the NSA have access to location data (I'm guessing the answer is no but would like assurances)?

All that said, this is an improvement over the status quo and over RuppRoge in several ways, not least that it applies only to phone data, and that they're using the same vocabulary we've just spent 10 months agreeing on common definitions for.

Update: One observation. One thing both this reform and RuppRoge include is the ability to dictate what the government gets from providers. That's a testament to how poorly suited the Section 215 program has always been, because it could only ask for existing business records, and most telecoms (the likely exception is AT&T) could and almost certainly did simply provide their SS7 telecom records, which would include everything, including cell location data that apparently became problematic, probably since 2010, when Congress learned NSA was actually going to start using that data. Those problems likely grew more intense after the Jones decision made it clear SCOTUS had problems with the government tracking location persistently without a warrant.

In other words, these "reforms" seem to arise as much from the fact that the outrage against this

dragnet provides the government with an opportunity to build a system more appropriate to the task at hand rather than what they could jerry-rig together in secret.

DOJ'S MULTIPLE AUTHORITIES FOR DESTROYING EVIDENCE

It seems like aeons ago, but just a week ago, EFF and DOJ had a court hearing over preserving evidence in the EFF lawsuits (Shubert, Jewel, and First Unitarian Church v. NSA). As I noted in two posts, a week ago Monday DOJ surprised EFF with the news that it had been following its own preservation plan, which it had submitted ex parte to Vaughn Walker, rather than the order Walker subsequently imposed. As a result, it has been aging off data in those programs (notably the PATRIOT-authorized Internet and phone dragnets) authorized by law, as opposed to what it termed Presidential authorization. DOJ's behavior makes it clear that it is trying to justify treating some data differently by claiming it was collected under different authorities.

Remember, there are at least five different legal regimes involved in the metadata dragnet:

- EO 12333 authority for data going back to at least 1998
- Stellar Wind authority lasting until 2004, 2006, and 2007 for different practices
- PATRIOT-authorized authorities for Internet (until 2011) and phone

records (until RuppRoge or something else passes)
- SPCMA, which is a subset of EO 12333 authority that conducts potentially problematic contact chaining integrating US person Internet metadata
- Five Eyes, which is EO 12333, but may involve GCHQ equities or, especially, ownership of the data

At the hearing and in their motions, EFF argued that their existing suits are not limited to any particular program (they didn't name all these authorities, but they could have). Rather, they are about the act of dragnetting, regardless of what authority (so they'll still be live suits after RuppRoge passes, for example).

EFF appears to have at least partly convinced Judge Jeffrey White, because on Friday he largely sided with EFF, extending the preservation order and — best as I can tell — endorsing EFF's argument that their suits cover the act of dragnetting, rather than just the Stellar Wind, FISA Amendments Act, or phone and Internet dragnets.

With that as background, I want to look at a few things from the transcript of last Wednesday's hearing. First, at one point White suggested there might be a — purely hypothetical, mind you — event that happened 5 years ago the plaintiffs might need live data from.

> THE COURT: Well, what if the NSA was doing something, say, five years ago that was broader in scope, and more problematical from the constitutional perspective, and those documents are now aged out? And — because now under the FISC or the orders

> > of the FISC Court, the activities of the NSA have – I mean, again, this is all hypothetical – have narrowed. And wouldn't the Government – wouldn't the plaintiffs then be deprived of that evidence, if it existed, of a broader, maybe more constitutionally problematic evidence, if you will?
>
> MR. GILLIGAN: There – we submit a twofold answer to that, Your Honor.
>
> We submit that there are documents that – and this goes to Your Honor's Question 5B, perhaps. There are documents that could shed light on the Plaintiffs' standing, whether we've actually collected information about their communications, even in the absence of those data.
>
> As far as – as Your Honor's hypothetical goes, it's a question that I am very hesitant to discuss on the public record; but I can say if this is something that the Court wishes to explore, we could we could make a further classified ex parte submission to Your Honor on that point.

Of course, this is not at all hypothetical. By NSA's own admission, they were watchlisting 3,000 US persons until just over 5 years ago without the requisite First Amendment review. And Theresa Shea has submitted another sealed filing in the suit, so White may know that. (Or maybe he reads yours truly – I believe I still am the only person to have reported this, though

it is in public records). Now, White doesn't hint at this, but this concern would already implicate two authorities, because the US persons were watchlisted under EO 12333 authorities (possibly SPCMA), dumped into Section 215 data, then moved back onto the EO 12333 lists.

Then there are a few ridiculous, more general claims. DOJ claimed it would take the most advanced SIGINT Agency in the world "many months" and hours of personnel time and technological resources to figure out how to save data onto a storage medium.

> Because we're talking about a periodic transition of data from the operational database to a preservation medium, we've got to develop a capability to do that, which is going to require a software-development effort that could take many months, and involve a diversion of many NSA resources.

EFF's Cindy Cohn noted, these claims of hardship are particularly odd given that the NSA proposed keeping all the data before the FISA Court.

> I'm a little confused about why they're fighting in front of you for the very thing they asked for in the FISC. They didn't talk about operational problems or difficulties preserving it when they asked the FISC for permission for this on March 7.

Judge White not only mocked this in the hearing, he basically extended the preservation order.

> MR. GILLIGAN: I think the answer to this question, Your Honor, brings us back to the discussion we were having with respect to your first question. The — migrating the data to tape would require, because we're dealing here with a live program, where data are coming in and data are periodically being aged

> off, rather than a program that has been terminated, and you have a static data set, you're going to have to or the NSA is going to have to engage in a complicated software-development effort to basically come up with a capability of periodically aging data off from the operational database into a preservation medium.
>
> THE COURT: But you're not saying the NSA, with all of its computer expertise, can't do this. You're not saying it's impossible to do it. You're saying it would be a burden financially and perhaps operationally, but it can be done; can it not?
>
> MR. GILLIGAN: Your Honor, we have not said it can't be done. If it – but again, it would be at significant costs that are detailed in classified declaration, and would result in a diversion of financial, technological, and personnel resources from the NSA's core national-security mission.

Then DOJ argued – in a lawsuit brought, in part, because the government has utterly blown up the definition of relevant – that relevance must be defined very narrowly here.

> Is this relevant evidence that is so potentially beneficial to the Plaintiffs' case, that preservation is required, notwithstanding the burden of doing so?
>
> We – we – simply ascertaining that the data are relevant within the meaning of the Rule 26 is only the start of the inquiry. It's not – it doesn't get us the answer to the question.

On both of these, you see how the multiple authorities involved could make the issue more difficult. EO 12333 data may not have age off

dates, 215 query **results** definitely don't, and GCHQ won't want to do anything with their data because our government is being sued. And one way to make all of this easier is to define relevance to those programs that FISC has authority over.

I'm most interested in the following exchange:

> This Court's jurisdiction is to determine what our preservation obligation is; but apart from preserving data, **what access we should have to it is something that should be determined by the FISC, and in accordance with statutes and regulations and Executives Orders that otherwise govern such matters**.
>
> THE COURT: On minimization?
>
> MR. GILLIGAN: On minimization, yes. Principally, minimization; **but perhaps otherwise**. The other thing that troubles us in this language is that I could foresee, particularly after the debate we've been having today, all in good faith, that we could find ourselves here three or four years down the road, arguing whether or not this language imposed some sort of independent restriction on the Government's access to preserve[d] data, which it absolutely should not do. Why – the Court's writ here is to tell us whether or not to preserve; **but what access we should have to our own data while it's being preserved is something, again, that is not at issue in this litigation**.
>
> [snip]
>
> MR. GILLIGAN: It would – within – any access we should have to that aged-out data would have to be with the permission of the FISC, and in accordance with FISC orders. The language here, Your Honor, I don't believe accomplishes the objective that

> Ms. Cohn just described. I'm either misunderstanding the language, or I'm misunderstanding Ms. Cohn's explanation of it. It says nothing in this order — this is language that Plaintiffs would have this Court enter — nothing in this order where the Court's prior preservation orders shall be construed as authorizing any review or use of telephone orders records or intelligence gathering for any other nonlitigation purposes. What we fear is that this — **we don't want sort of a day to come where there's an argument that this language independently barred us from accessing the data**. Any restrictions on our access to the data are — should be imposed by the FISC in accordance with the terms of FISA. To the extent that that —
>
> THE COURT: So it's a jurisdictional issue, is really what you're saying?
>
> MR. GILLIGAN: Right. The Congress, through FISA, conferred on the FISC the authority to determine whether and under what circumstances the particular personnel should have access to data that are acquired under the authority of FISA.

The same DOJ that has agreed in FISC to not touch any data archived for this preservation order is here saying that White can't impose any such order because it's their data damnit and they can access it if they want to!

It's a seeming contradiction.

Except it's not, not even for the Section 215 data, because the data in question may well be in the corporate store! That data would be the most important to show the plaintiffs' exposure.

Moreover, there's all the other data — the 12333, the SPCMA, GCHQ's own data — that they have limited restrictions on accessing, each having also fed the corporate store.

But here's the thing: The government got White not to impose this protection order here based on a claim that it falls under FISC's jurisdiction. And that's true for the small fraction of it that derives from Section 215. But the bulk of it doesn't arise from 215, it arises from 12333.

Which is, in part, what Gilligan was referring to when he raised "statutes and regulations and Executives Orders." Except that for that data, White should be entitled to jurisdiction because FISA doesn't.

Meanwhile, DOJ wants to delete the legally collected stuff and keep playing with the rest of it.

NSA BIDS TO EXPAND SPYING IN GUISE OF "FIXING" PHONE DRAGNET

Dutch Ruppersberger has provided Siobhan Gorman with details of his plan to "fix" the dragnet — including repeating the laughable claim that the "dragnet" (which she again doesn't distinguish as solely the Section 215 data that makes up a small part of the larger dragnet) doesn't include cell data.

Only, predictably, it's not a "fix" of the phone dragnet at all, except insofar as NSA appears to be bidding to use it to do all the things they want to do with domestic dragnets but haven't been able to do legally. Rather, it appears to be an attempt to outsource to telecoms some of the things the NSA hasn't been able to do legally since 2009.

For example, there's the alert system that

Reggie Walton shut down in 2009.

As I reported back in February, the NSA reportedly has never succeeded in replacing that alert system, either for technical or legal reasons or both.

> NSA reportedly can't get its automated chaining program to work. In the motion to amend, footnote 12 — which modifies part of some entirely redacted paragraphs describing its new automated alert approved back in 2012 — reads:
>
> > 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.
>
> PCLOB describes this automated alert this way.
>
> > 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."
>
> It has been 15 months since FISC approved this alert, but NSA still can't get it working.
>
> I suspect this is the root of the stories claiming NSA can only access 30% of US phone records.

As described by WSJ, this automated system will be built into the orders NSA provides telecoms; once a selector has been provided to the telecoms, they will keep automatically alerting on it.

> Under the new bill, a phone company would search its databases for a phone number under an individual "directive" it would receive from the government. It would send the NSA a list of numbers called from that phone number, and possibly lists of phone numbers those numbers had called. **A directive also could order a phone company to search its database for such calls as future records come in**. [my emphasis]

This would, presumably, mean NSA still ends up with a corporate store, a collection of people against whom the NSA has absolutely not a shred of non-contact evidence, against whom they can use all their analytical toys, including searching of content.

Note, too, that this program uses the word

“directive,” not query. Directive comes from the PRISM program, where the NSA gives providers generalized descriptions and from there have broad leeway to add new selectors. Until I hear differently, I’ll assume the same is true here: that this actually involves less individualized review before engaging in 2 degrees of Osama bin Laden.

The legislation seems ripe for inclusion of querying of Internet data (another area where the NSA could never do what it wanted to legally after 2009), given that it ties this program to “banning” (US collection of, but Gorman doesn’t say that either, maintaining her consistency in totally ignoring that EO 12333 collection makes up the greater part of bulk programs) Internet bulk data collection.

> The bill from Intelligence Committee Chairman Mike Rogers (R., Mich.) and his Democratic counterpart, Rep. C.A. “Dutch” Ruppersberger (D., Md.), would ban so-called bulk collection of phone, email and **Internet** records by the government, according to congressional aides familiar with the negotiations. [my emphasis]

Call me crazy, but I’m betting there’s a way they’ll spin this to add in Internet chaining with this “fix.”

Note, too, Gorman makes no mention of location data, in spite of having tied that to her claims that NSA only collects 20% of data. Particularly given that AT&T’s Hemisphere program provides location data, we should assume this program could too, which would present a very broad expansion on the status quo.

And finally, note that neither the passage I quoted above on directives to providers, nor this passage specifies what kind of investigations this would be tied to (though they are honest that they want to do away with the fig leaf of this being tied to

investigations at all).

> The House intelligence committee bill doesn't require a request be part of an ongoing investigation, Mr. Ruppersberger said, because intelligence probes aim to uncover what should be investigated, not what already is under investigation.

Again, the word "directive" in the PRISM context also provides the government the ability to secretly pass new areas of queries — having expanded at least from counterterrorism to counterproliferation and cybersecurity uses. So absent some very restrictive language, I would assume that's what would happen here: NSA would pass it in the name of terrorism, but then use it primarily for cybersecurity and counterintelligence, which the NSA considers bigger threats these days.

And that last suspicion? That's precisely what Keith Alexander said he planned to do with this "fix," presumably during the period when he was crafting this "fix" with NSA's local Congressman: throw civil libertarians a sop but getting instead an expansion of his cybersecurity authorities.

Update: Here's Spencer on HPSCI, confirming it's as shitty as I expected.

And here's Charlie Savage on Obama's alternative.

It would:

- Keep Section 215 in place, though perhaps with limits on whether it can be used in this narrow application
- Enact the same alert-based system and feed into the corporate store, just as the HPSCI proposal would
- Include judicial review like

> they have now (presumably including automatic approval for FISA targets)

Obama's is far better than HPSCI (though this seems to be part of a bad cop-good cop plan, and the devil remains in the details). But there are still some very serious concerns.

IN NOMINATION HEARING, DIRNSA NOMINEE MIKE ROGERS CONTINUES JAMES CLAPPER AND KEITH ALEXANDER'S OBFUSCATION ABOUT BACK DOOR SEARCHES

Yesterday, the Senate Armed Services Committee held a hearing for Vice Admiral Mike Rogers to serve as head of Cyber Command (see this story from Spencer about how Rogers' confirmation as Cyber Command chief serves as proxy for his role as Director of National Security Agency because the latter does not require Senate approval).

Many of the questions were about Cyber Command (which was, after all, the topic of the hearing), but a few Senators asked questions about the dragnet that affects us all.

In one of those exchanges — with Mark Udall — Rogers made it clear that he intends to continue to hide the answers to very basic questions about how NSA conducts warrantless surveillance of Americans, such as whether the NSA conducts

back door searches on American people.

> Udall: If I might, in looking ahead, I want to turn to the 702 program and ask a policy question about the authorities under Section 702 that's written into the FISA Amendments Act. The Committee asked your understanding of the legal rationale for NASA [sic] to search through data acquired under Section 702 using US person identifiers without probable cause. You replied the NASA—the NSA's court approved procedures only permit searches of this lawfully acquired data using US person identifiers for valid foreign intelligence purposes and under the oversight of the Justice Department and the DNI. The statute's written to anticipate the incidental collection of Americans' communications in the course of collecting the communications of foreigners reasonably believed to be located overseas. But the focus of that collection is clearly intended to be foreigners' communications, not Americans. But declassified court documents show that in 2011 the NSA sought and obtained the authority to go through communications collected under Section 702 and conduct warrantless searches for the communications of specific Americans. Now, my question is simple. **Have any of those searches been conducted?**
>
> Rogers: I apologize Sir, **I'm not in a position to answer that as the nominee.**
>
> Udall: You—yes.
>
> Rogers: But if you would like me to come back to you in the future if confirmed to be able to specifically address that question I will be glad to do so, Sir.
>
> Udall: Let me follow up on that. You may recall that Director Clapper was asked

> this question in a hearing earlier this year and he didn't believe that an open forum was the appropriate setting in which to discuss these issues. The problem that I have, Senator Wyden's had, and others is that we've tried in various ways to get an unclassified answer – simple answer, yes or no – to the question. We want to have an answer because it relates – the answer does – to Americans' privacy. **Can you commit to answering the question before the Committee votes on your nomination?**
>
> Rogers: Sir, I believe that one of my challenges as the Director, if confirmed, is how do we engage the American people – and by extension their representatives – in a dialogue in which they have a level of comfort as to what we are doing and why. That is no insignificant challenge for those of us with an intelligence background, to be honest. But I believe that one of the takeaways from the situation over the last few months has been as an intelligence professional, as a senior intelligence leader, I have to be capable of communicating in a way that we are doing and why to the greatest extent possible. That perhaps the compromise is, **if it comes to the how we do things, and the specifics, those are perhaps best addressed in classified sessions,** but that one of my challenges is I have to be able to speak in broad terms in a way that most people can understand. And I look forward to that challenge.
>
> Udall: I'm going to continue asking that question and I look forward to working with you to rebuild the confidence. [my emphasis]

The answer to the question Rogers refused to answer is clearly yes. We know that's true

because the answer is always yes when Wyden, and now Udall, ask such questions.

But we also know the answer is yes because declassified parts of last August's Semiannual Section 702 Compliance Report state clearly that oversight teams have reviewed the use of this provision, which means there's something to review.

> As reported in the last semiannual assessment, NSA minimization procedures now permit NSA to query its databases containing telephony and non-upstream electronic communications using United States person identifiers in a manner designed to find foreign intelligence information. Similarly, CIA's minimization procedures have been modified to make explicit that CIA may also query its databases using United States person identifiers to yield foreign intelligence information. As discussed above in the descriptions of the joint oversight team's efforts at each agency, **the joint oversight team conducts reviews of each agency's use of its ability to query using United States person identifiers.** To date, this review has not identified any incidents of noncompliance with respect to the use of United States person identifiers; as discussed in Section 4, the agencies' internal oversight programs have, however, identified isolated instances in which Section 702 queries were inadvertently conducted using United States person identifiers. [my emphasis]

It even obliquely suggests there have been "inadvertent" violations, though this seems to entail back door searches on US person identifiers without realizing they were US person identifiers, not violations of the procedures for using back door searches on identifiers known to be US person identifiers.

Still, it is an unclassified fact that NSA uses these back door searches.

Yet the nominee to head the NSA refuses to answer a question on whether or not NSA uses these back door searches.

And it's not just in response to this very basic question that Rogers channeled the dishonest approach of James Clapper and Keith Alexander.

As Udall alluded, at the end of a long series of questions about Cyber Command, the committee asked a series of questions about back door searches and other dragnet issues. They asked (see pages 42-43):

- Whether NSA can conduct back door searches on data acquired under EO 12333 and if so under what legal rationale
- Whether NSA can conduct back door searches on data acquired pursuant to traditional FISA and if so under what legal rationale
- What the legal rationale is for back door searches on data acquired under FISA Amendments Act
- What the legal rationale is for searches on the Section 215 query results in the "corporate store"

I believe every single one of Rogers' answers — save perhaps the question on traditional FISA — involves some level of obfuscation. (See this post for further background on what NSA's Raj De and ODNI's Robert Litt have admitted about back door searches.)

Consider his answer on searches of the

"corporate store" as one example.

> **What is your understanding of the legal rationale for searching through the "Corporate Store" of metadata acquired under section 215 using U.S. Persons identifiers for foreign intelligence purposes?**
>
> The section 215 program is specifically authorized by orders issued by the Foreign Intelligence Surveillance Court pursuant to relevant statutory requirements. (Note: the legality of the program has been reviewed and approved by more than a dozen FISC judges on over 35 occasions since 2006.) As further required by statute, the program is also governed by minimization procedures adopted by the Attorney General an d approved by the FISC. Those orders, and the accompanying minimization procedures, require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization specified in the Court's order.

Remember, not only do declassified Primary Orders make it clear NSA doesn't need Reasonable Articulable Suspicion to search the corporate store, but PCLOB has explained the possible breadth of "corporate store" searches plainly.

> 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

There is no debate over whether NSA can conduct back door searches in the "corporate store" because both FISC and PCLOB say they can.

Which is probably why SASC did not ask **whether** this was possible — it is an unclassified fact that it is — but rather what the legal rationale for doing so is.

And Rogers chose to answer this way:

1. By asserting that the phone dragnet must comply with statutory requirements
2. By repeating tired boilerplate about how many judges have approved this program (ignoring that almost all of these approvals came before FISC wrote its first legal opinion on the program)
3. By pointing to AG-approved minimization procedures

(note—it's not actually clear that NSA's — as distinct from FBI's — dragnet specific procedures are AG-approved, though the more general USSID 18 ones are)

4. By claiming FISA orders and minimization procedures "require that searches of data under the program may only be performed when there is a Reasonable Articulable Suspicion that the identifier to be queried is associated with a terrorist organization"

The last part of this answer is either downright ignorant (though I find that unlikely given how closely nominee responses get vetted) or plainly non-responsive. The question was not about queries of the dragnet itself — the "collection store" of all the data. The question was about the "corporate store" — the database of query results based off those RAS approved identifiers. And, as I said, there is no dispute that searches of the corporate store do not require RAS approval. In fact, the FISC orders Rogers points to say as much explicitly.

And yet the man Obama has picked to replace Keith Alexander, who has so badly discredited the Agency with his parade of lies, refused to answer that question directly. Much less explain the legal rationale used to conduct RAS-free searches on phone query results showing 3rd degree connections to someone who might have ties to terrorist groups, which is what the question was.

Which, I suppose, tells us all we need to know about whether anyone plans to improve the

credibility or transparency of the NSA.

CONGRESS CURRENTLY HAS ACCESS TO THE PHONE DRAGNET QUERY RESULTS

When Bernie Sanders asked the NSA whether it spied on Members of Congress, Keith Alexander responded, in part,

> Among those protections is the condition that NSA can query the metadata only based on phone numbers reasonably suspected to be associated with specific foreign terrorist groups. For that reason, NSA cannot lawfully search to determine if any records NSA has received under the program have included metadata of the phone calls of any member of Congress, other American elected officials, or any other American without that predicate.

Alexander's response was dated January 10, 2014, one week after the current dragnet order was signed.

It's an interesting response, because one of the changes made to the dragnet access rules with the January 3 order was to provide Congress access to the data for oversight reasons. Paragraph 3D reads, in part,

> Notwithstanding the above requirements, NSA may share the results from intelligence analysis queries of the BR metadata, including United States person information, with Legislative Branch personnel to facilitate lawful oversight

> functions.

This doesn't actually mean Sanders (and Darrell Issa, Jerrold Nadler, and Jim Sensenbrenner, who sent a letter on just this issue yesterday) can just query up the database to find out if their records are in there. The legislature can only get query results — it can't perform queries. And as of last week, all query identifiers have to be approved by the FISC.

Still, they might legitimately ask to see what is in the corporate store, the database including some or all past query results, which may include hundreds of millions of Americans' call records. And Nadler and Sensenbrenner — as members of the Judiciary Committee — can legitimately claim to play an oversight role over the dragnet.

So why don't they just ask to shop the corporate store, complete with all the US person data, as permitted by this dragnet order? While they're at it, why not check to see if the 6 McClatchy journalists whose FOIA NSA just rejected have been dumped into the corporate store? (No, I don't think giving Congress this access is wise, but since they have it, why not use it?)

Incidentally, this access for legislative personnel is not unprecedented. Starting on February 25, 2010 and lasting through 3 orders (so until October 29, 2010, though someone should check my work on this point) the dragnet orders included even broader language.

> Notwithstanding the above requirements, NSA may share certain information, as appropriate, derived from the BR metadata, including U.S. person identifying information, with Executive Branch and Legislative Branch personnel in order to enable them to fulfill their lawful oversight functions…

Of course at that point, most of Congress had no real understanding of what the dragnet is.

Now that they do, Nadler and Sensenbrenner should use the clear provision of the dragnet order as an opportunity to develop a better understanding of what happens to query results and how broadly they implicate average Americans' privacy.

Update: Added short explanation of corporate store.

OMAHA! OMAHA! THE ALERT THAT WON'T ALERT

The FISA Court just released the January 3, 2014 phone dragnet order, DOJ's motion to amend it to meet Obama's new dragnet terms, and the approval for that.

But those changes are of the least interest in these documents. I'll explain the loophole to the changes tomorrow.

For now, consider that the NSA reportedly can't get its automated chaining program to work. In the motion to amend, footnote 12 — which modifies part of some entirely redacted paragraphs describing its new automated alert approved back in 2012 — reads:

> 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.

PCLOB describes this automated alert this way.

> 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."

It has been 15 months since FISC approved this alert, but NSA still can't get it working.

I suspect this is the root of the stories claiming NSA can only access 30% of US phone records.

And I think it probably does have to do with cell data and what they get from other programs — just not in the way the reports said it did.

I'll explain that in a follow-up.

THE "FOREIGN INTELLIGENCE"

DRAGNET MAY NOT BE ABOUT "FOREIGN INTELLIGENCE"

There's one more totally weedy change in the phone dragnet orders I wanted to point out: the flimsy way the program has, over time, tied into "foreign intelligence."

To follow along, it's helpful to use the searchable versions of the phone dragnet orders ACLU has posted.

Start by searching on this order — from December 11, 2008, just before FISC started cleaning up the dragnet problems — for "foreign intelligence" (all the earlier orders are, I believe, identical in this respect). You should find 5 instances: 3 references to the FISC, a reference to the language from the Section 215 statute requiring the tangible things be **either** for foreign intelligence **or** to protect against international terrorism (¶1 on page 2), and a discussion tying dissemination of US person data to understanding foreign intelligence (¶(3)D on page 9).

In the last instance, the order introduces foreign intelligence, but then drops it. The very next sentence shifts the measure of whether the US person information can be disseminated from "foreign intelligence" to "counterterrorism" — and counterterrorism here is **not** explicitly tied to international terrorism, although the statute requires it to be.

> Before information identifying a U.S. person may be disseminated outside of NSA, a judgment must be made that the identity of the U.S. person is necessary to understand the foreign intelligence information or to assess its importance. Prior to the dissemination of any U.S. person identifying information, the Chief of Information Sharing Services in

> the Signals Intelligence Directorate must determine 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.

Significantly, ¶(3)C on page 8 — the main paragraph restricting NSA's access to the dragnet data — says nothing about foreign intelligence.

This language would, I believe, have permitted the government to search on and disseminate US person information for reasons without a foreign nexus (and they played word games with other language in the original orders, notably with the word "archives").

Now check out the next order, dated March 5, 2009. In this — the first of the primary orders dealing with the dragnet problems — the language potentially tying the FBI investigation to foreign intelligence is eliminated (I talked about that change here).The language on dissemination remains the same — that is, the paragraph does not tie dissemination of US person information to terrorism with an international nexus. But ¶(3)C — the key paragraph regulating access — now specifies that NSA can only "query the BR metadata for purposes of obtaining foreign intelligence."

In the process of very narrowly limiting what NSA could do with the phone dragnet, Judge Reggie Walton added language limiting queries to foreign intelligence purposes, not just terrorism purposes (though I believe it still could be read as permitting dissemination of information without a foreign nexus).

As a reminder, during the interim period, the government had admitted to tracking 3,000 US persons without submitting them to a First Amendment review.

The orders for the following year changed

regularly (and the Administration has withheld what are surely the most interesting orders from that year), but they retained that restriction on queries to foreign intelligence purposes.

But now look what that language in ¶(3)C has since evolved into, starting with the order dated October 29, 2010, though the language below comes from the April 25, 2013 order (the October 29 one has "raw data" hand-written into it, making it clear these requirements, including auditability, only applies to the collection store, not the corporate store).

> NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata as described in paragraph 17 of the [redacted] Declaration attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.5 NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.

At first glance, this paragraph would seem to add protections that weren't in the orders previously, ensuring that the phone dragnet only be accessed for foreign, not domestic, intelligence.

But it's actually only partly a protection.

In fact, the "foreign intelligence" language here serves to distinguish this controlled access from the "data integrity" access (though

they no longer call it that), which is described in the previous paragraph.

> Appropriately trained and authorized tedmical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms4 that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes, but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, i.e., the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any 9f NSA' s various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

Footnote 4, discussing "selection terms" is a fairly long, entirely redacted paragraph. And the last sentence, allowing these technical personnel to **also** conduct foreign intelligence information queries, is fairly recent.

This language would seem to describe the data integrity role more than it had previously been, specifying the search for high volume numbers,

plus whatever appears in footnote 4. And it would seem to limit the use of such information, since it doesn't permit "intelligence analysis" (notwithstanding the fact that figuring out which selectors are high volume **is** intelligence analysis, to say nothing about the underlying technical decisions that shape automated search functions). But the **first** use of the dragnet in current descriptions pertains not to contact chaining at all, but as a resource for tech personnel to identify certain characteristics of call patterns using raw data.

Further, these tech personnel now get to double dip: access raw data in intelligible form to get it ready for querying and something else, and access it to conduct queries. That they even have that authority — explicitly — ought to raise alarm bells. Anything data integrity analysts see while doing data integrity, they can run as a query to access in a form that can be disseminated.

Now, perhaps this alarming structural issue is not being abused or exploited. Perhaps it shouldn't concern us that a dragnet purportedly serving "foreign intelligence" purposes seems to serve, even before that, a different role entirely, not only tied to any foreign purpose.

But we have had assurances over and over in the last 8 months that the NSA can only access this database for certain narrowly defined foreign intelligence purposes. That wasn't, by letter of the order, at least, true for the first three years. And by the letter of the order, it's not true now.

ANCIENT HISTORY: DECEMBER 2012 IN THE

DRAGNET

PCLOB tells us that the FISA Court approved a new automated query system (versions appear to have been in development for years, and it replaced the automated alert system from 2009) in late 2012 that permitted all the 3-degree contact chains off all RAS-approved identifiers to be dumped into the corporate store at once where they can be combined with data collected under other authorities (presumably including both EO 12333 and FAA) for further analysis.

> 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 perform s 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.
>
> 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.

(While I didn't know the date, I have been pointing the extent to which corporate store data can be analyzed for some time, but thankfully the PCLOB report has finally led others to take notice.)

On December 27, 2012, Jeff Merkley gave a speech in support of his amendment to the FISA Amendments Act that would push to make FISC decisions public. It referenced both the backdoor loophole (which John Bates extended to NSA and CIA in 2011, was implemented in 2012, and affirmed by the Senate Intelligence Committee in June 2012) **and** the language underlying the phone dragnet. Merkley suggested the government might use these secret interpretations to conduct wide open spying on Americans.

> If it is possible that our intelligence agencies are using the law to collect and use the communications of Americans without a warrant, that is a problem. Of

> course, we cannot reach conclusions about that in this forum because this is an unclassified discussion.
>
> My colleagues Senator Wyden and Senator Udall, who serve on Intelligence, have discussed the loophole in the current law that allows the potential of backdoor searches. **This could allow the government to effectively use warrantless searches for law-abiding Americans**. Senator Wyden has an amendment that relates to closing that loophole. Congress never intended the intelligence community to have a huge database to sift through without first getting a regular probable cause warrant, but because we do not have the details of exactly how this proceeds and we cannot debate in a public forum those details, then we are stuck with wrestling with the fact that we need to have the sorts of protections and efforts to close loopholes that Senator Wyden has put forward.
>
> [snip]
>
> Let me show an example of a passage. Here is a passage about what information can be collected: " ….. reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2)," and so on.
>
> Let me stress these words: "relevant to an authorized investigation."
>
> There are ongoing investigations, multitude investigations about the conduct of individuals and groups around this planet, and one could make the argument that any information in the world helps frame an understanding of what these foreign groups are doing. So

> certainly there has been some FISA Court decision about what "relevant to an authorized investigation" means or what "tangible things" means. **Is this a gateway that is thrown wide open to any level of spying on Americans or is it not?** Is it tightly constrained in understanding what this balance of the fourth amendment is? We do not know the answer to that. We should be able to know. If we believe that an administration and the secret court have gone in a direction incompatible with our understanding of what we were seeking to defend, then that would enable us to have that debate here about whether we tighten the language of the law in accordance with such an interpretation. **Again, is this an open gateway to any information anywhere in the world, anytime, on anyone or is it a very narrow gate? We do not know.** [my emphasis]

Also in December 2012, the White House wrote a set of talking points warning, in part, that if Congress aligned the expiration dates of FAA with the PATRIOT Act it might lead some people to think they were connected.

> Aligning FAA with expiration of provisions of the Patriot Act risks confusing distinct issues.

Now why is it, do you think, that the White House was so worried, when it was refusing to release information about either the backdoor loophole or the phone dragnet that serves as an index to tell NSA which content to access, that we might think PATRIOT had some tie to FAA?

The relationship between the dragnet and content has, as NSA's SID Director Theresa Shea represented in declarations last year, been in place for some time. But it sure seems like it got new life in 2012, just as the Administration

got Congress to reauthorize one half of the whole contraption.