THE GOVERNMENT USES THE DRAGNETS FOR DETAINEE PROCEEDINGS

In the middle of a discussion of how the NSA let FBI, CIA, and NCTC directly access the database of Internet query results in the report accompanying the Internet dragnet End-to-End report, a footnote describes searches NSA's litigation support team conducts. (See page 12)

> In addition to the above practices, NSA's litigation support team conducts prudential searches in response to requests from Department of Justice or Department of Defense personnel in connection with criminal or detainee proceedings. The team does not perform queries of the PR/TT metadata. This practice of sharing information derived from PR/TT metadata was later specifically authorized. See Primary Order, Docket Number PR/TT [redacted] at 12-13. The Government respectfully submits that NSA's historic practice of sharing of U.S. person identifying information in this manner before it was specifically authorized does not constitute non-compliance with the PR/TT Orders.

Keith Alexander's declaration accompanying the E2E adds more detail. (See page 16)

> The designated approving official does not make a determination to release information in response to requests by Department of Justice or Department of Defense personnel in connection with criminal or detainee proceedings. In the case of such requests, NSA's Litigation Support Team conducts prudential, specific searches of databases that contain both previously disseminated

> reporting and related analyst notes. The team does not perform queries of the PR/TT metadata. NSA then provides that research to Department of Justice or Department of Defense personnel for their review in connection with criminal or detainee proceedings. This practice of sharing information derived from the PR/TT metadata is now specifically authorized. *See* Primary Order, Docket Number PR/TT [redacted] at 12-13.

Language approving searches of the corporate store conducted on behalf of DOJ and DOD does not appear (at least not at 12-13) in the early 2009 — probably March 2, 2009 — Internet dragnet primary order. But related language was included in the September 3, 2009 phone dragnet order (it does not appear in the July 8, 2009 phone dragnet order, so that appears to have been the first approval for it). Given the timing, the language might stem either from another notice of violation to the FISC (one the government has redacted thus far); or, it might be a response to recommendations made in the Joint IG Report on the illegal dragnet, which was released July 10, 2009, and which did discuss discovery problems.

But the language describing the Litigation Support Team searches is far less descriptive in the September 3, 2009 phone dragnet order.

> Notwithstanding the above requirements, NSA may share information derived from the BR metadata, including U.S. person identifying information, with Executive Branch personnel in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings.

The E2E and Alexander's declaration make two things more clear.

First, NSA can disseminate this information without declaring the information is related to counterterrorism (that's the primary dissemination limitation discussed in this section), and of course, without masking US person information. That would at least permit the possibility this data gets used for non-counterterrorism purposes, but only when it should least be permitted to, for criminal prosecutions of Americans!

Remember, too, the government has explicitly said it uses the phone dragnet to identify potential informants. Having non-counterterrorism data available to coerce cooperation would make that easier.

The E2E and Alexander declaration also reveal that the Litigation Support Team conducts these searches not just for DOJ, but also for DOD on detainee matters.

That troubles me.

According to the NYT's timeline, only 20 detainees arrived at Gitmo after these dragnets got started, and 14 of those were High Value Detainees who had been stashed elsewhere for years (as were the last batch arrived in 2004). None of the men still detained at Gitmo, at least, had been communicating with anyone outside of very closely monitored situations for years. None of the Internet dragnet data could capture them (because no historical data gets collected). And what phone data might include them — and remember, the phone dragnet was only supposed to include calls with one end in the US — would be very dated.

So what *would* DOD be using these dragnets for?

Perhaps the detainees in question weren't Gitmo detainees but Bagram detainees. Plenty of them had been out communicating more recently in 2004 and 2006 and even 2009, and their conversations might have been picked up on an Internet dragnet (though I find it unlikely any were making phone calls to the US).

It’s possible the dragnet was used, in part, to track released detainees. Is dragnet contact chaining one of the things that goes into claims about “recidivist” detainees?

Finally, a more troubling possibility is that detainee attorneys’ contacts with possible witnesses got tracked. Is it possible, for example, that DOD tracked attorneys’ contacts with detainee family members in places like Yemen? Given allegations the government spied on detainees’ lawyers, that’s certainly plausible. Moreover, since NSA does not minimize contacts between attorneys and their client until the client has been indicted, and so few of the Gitmo detainees have been charged, it would be utterly consistent to use the dragnet to track lawyers’ efforts to defend Gitmo detainees. Have the dragnets been focused on attorneys all this time?

One thing is clear. There is not a single known case where DOJ or DOD have used the dragnets to provide exculpatory information to someone; Dzhokhar Tsarnaev was unable to obtain discovery on dragnet information even after the government bragged about using the dragnet in his case.

Nevertheless, NSA has been sharing US person information without even having to attest it is counterterrorism related, outside of all the minimization procedures the government boasts about.

WORKING THREAD, INTERNET DRAGNET 5: THE AUDACIOUS 2010 REAPPLICATION

At some point (perhaps at the end of 2009, but sometime before this application), the

government tried to reapply, but withdrew their application. The three letters below were sent in response to that. But they were submitted with the reapplication.

*See also **Working Thread 1**, **Working Thread 2**, **Working Thread 3**, Working Thread 4, and **Internet Dragnet Timeline**. No one else is doing this tedious work; if you find it useful, **please support it**.*

U. **First Letter in Response to FISC Questions Concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**,

(15/27) In addition to tagging data itself, the source now gets noted in reports.

(16/27) NSA wanted all analysts to be able to query.

(16/27) COntrary to what redaction seemed to indicate elsewhere, only contact chaining will be permitted.

(17/27) This implies that even technical access creates a record, though not about what they access, just when and who did it.

(17/27) NSA asked for the same RAS timelines as in BRFISA — I think this ends up keeping RAS longer than an initial PRTT order.

(18/27) "Virtually every PR/TT record contains some metadata that was authorized for collection, and some metadata that was not authorized for collection … virtually every PR/TT record contains some data that was not authorized by prior orders and some that was not."

(21/27) No additional training for internal sharing of emails.

(21/27) Proof they argue everything that comes out of a query is relevant to terrorism:

> Results of queries of PR/TT-sourced metadata are inherently germane to the analysis of counterterrorism-related foreign intelligence targets. This is

> because of NSA's adherence to the RAS standard as a standard prerequisite for querying PR/TT metadata.

(22/27) Note "relevance" creep used to justify sharing everywhere. I really suspect this was built to authorize the SPCMA dragnet as well.

(23/27) Curious language about the 2nd stage marking: I think it's meant to suggest that there will be no additional protection once it circulates within the NSA.

(24/27) NSA has claimed they changed to the 5 year age-off in December 2009. Given the question about it I wonder if that's when these letters were sent?

(24/27) Their logic for switching to USSID-18:

> these procedures form the very backbone for virtually all of NSA's dissemination practices. For this reason, NSA believes a weekly dissemination report is no longer necessary.

(24-5/27) The explanation for getting rid of compliance meetings is not really compelling. Also note that they don't mention ODNI's involvement here.

(25/27) "effective compliance and oversight are not performed simply through meetings or spot checks."

(27/27) "See the attached word and pdf documents provided by OIG on an intended audit of PR/TT prior to the last Order expiring as an example." Guess this means the audit documents are from that shutdown period.

V. **Second Letter in Response to FISC Questions concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**,

W. **Third Letter in Response to FISC Questions Concerning NSA Bulk Metadata Collection Using Pen Register/Trap and Trace Devices**.

(2) DNI adopted new serial numbers for reports, so as to be able to recall requests.

(3) THey're tracking the query reports to see if they can withdraw everything.

(3) THis is another of the places they make it clear they can disseminate law enforcement information without the USSID requirements.

(4) It appears the initial application was longer than the July 2010, given the reference to pages 78-79.

Q: **Government's Application for Use of Pen Register/Trap and Trace Devices for Foreign Intelligence Purposes**. (around July 2010)

There are some very interesting comparisons with the early 2009 application, document AA.

(1) Holder applied directly this time rather than a designee (Holder may not have been confirmed yet for the early 2009 one).

(2) The redacted definition of foreign power in AA was longer.

(3) "collect" w/footnote 3 was redacted in AA.

(3) Takes out reference to "email" metadata.

(3) FN 4 both focuses on "Internet communication" rather than "email [redacted]" as AA did, but it also scopes out content in a nifty way.

(3) FN 5 appears to define "Internet comm."

(4) They add "databases and/or archives" though "archives" was only withdrawn from AA because Walton has just prohibited its use. Also, this uses "repositories" plural.

(4) Defined "identifiers" here used to be email [redacted].

(4) "As appropriate" language at bottom is new.

(5) THere was a footnote on "subject of any FBI investigation" in AA.

(5) “metadata” in middle of page used to be “data.”

(5) As with Holder, here Alexander replaces a surrogate in AA.

(5) This admits they will share with foreign governments; AA did not.

(6) In 2, “information” was “metadata,” and “collected” was “acquired.” Facilities (or its predecessor) redacted in AA.

(6) Govt didn’t submit memo of law w/AA.

(7) Govt didn’t include USSID 18 in AA.

(7) Note reference to April 2010 FBI number; in AA this was December 2008. Both seem to be about 3 months before the application.

(7) Last redaction is “the NSA” in AA.

(8) There’s a shift from talking about pen register devices (in AA) to talking about PR authority.

(9) No mention of “below the bcc line” which was in AA and original application.

(9) Unique markings is new—was added by Walton previous fall.

(9) Defeat list obv neW.

(12) The “auditible record” in AA was listed out.

(12) FN 10: this associated language is particularly important.

(13-14) The “DNI has independent responsibility” language is new, and does not have a parallel in the BR FISAs either before or after.

(14) The order on this compliance stuff has been tweaked a bit. Also, they replaced “shall” with “will” throughout.

(15) description of changes in methods is new

(15) Now they’ve switched back to talking about “devices” again.

(16) Obv this is all new.

R. **Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes**,

(2) They repeat—then add a long footnote—to their new definition of "not content."

(3) They've decided what they did before was all legal and therefore should be able to collect it all.

(4) The bid to getting rid of past minimization procedures is missing a comma.

(5) Note reference to single doc recovered (this would be before OBL killing).

(9) The "particularly importance" language may suggest "some" limits, but they're likely very small.

(11) Now they use "content" in the traditional fashion.

(14) They must not specify even all the locations they're collecting given the post-redaction sentence.

(15) Just some of the data will be subject to "multi-level validation" before going into the repositories.

(16) A long redaction before we get to the part of querying we're used to. Makes me think of the call-chaining prep as described earlier.

(21) Important discussion of how they changed this starts here: Note it probably explains the different language they used relating to collection versus acquiring.

(22) Here's where they do their DRAS =/= content.

(23) Once again the govt is speaking broadly about what Congress intended. I wonder whether this was timed to the 2010 reauthorization of PATRIOT?

(24) Here we go:

> Information that is both located in the appropriate field and is in the appropriate format for addressing is by definition 'addressing information.' Nothing in the pen register statutes requires "addressing information" to be used for the functional or technical purposes of addressing at the time of collection.

(25) They're also getting rambunctious with the definition of "facilities" but that's all redacted.

(29) Once again they argue the FISC has "limited' authority with respect to a PRTT application.

> The Government continues to believe that the language of the Certification should be determinative of this issue and incorporates those previously advanced arguments as if set forth more fully herein.

(30) This is one of my favorite comments from these documents.

> Relevance here is not properly measured through scientific metrics or the number of reports issued over the course of a year and it does not require a statistical "tight fit" between the volume of proposed collection and the much smaller proportion of information that will be directly "relevant" to the investigations of the Foriegn Powers to protect against international terrorism. *See* Opinion and Order, docket number PR/TT [redacted], at 49-50. Rather, relevance here properly is measure in packets of metadata that over an extended period of time, can help to fill in information that provides a more complete picture of the communications practices of these Foreign Powers and

> their agents.

(36) Lots of pretty unconvincing language in here as to whether this stuff really counts as DRAS.

(45) The discussion in footnote 25 has an error in the reference to the House Report, which should go back to the earlier referenced one. Here's the discussion that is redacted.

> Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order could not be used to collect information other than '' dialing, routing, addressing, and signaling'' information, such as the the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.
>
> This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, applies across the board to all communications media, and to actual connections as well as attempted connections (such as busy signals and similar signals in the telephone context and packetsthat merely request a telnet connection in the Internet context).

(46) They distinguish between this and the information in a pager.

(46) Wonder what the subject of the District Court opinions are: location?

(50) In footnote 28, the government dismisses language prohibiting the collection of other stuff as irrelevant to their question of whether they can collect stuff that's not DRAS but allegedly not content.

(55) I think they have redacted some, but not

all, of the email “validation” references elsewhere.

(56) The redacted stuff must get closer to admitting this stuff is meaningful content.

(59) The government counterposes “individualized warrant” against collecting all metadata.

(60) I’d be curious whether the Kerr citation treats the same stuff they’re saying isn’t content.

(62) Really curious redaction in FN 33. Especially since I believe FISC changed minimization procedures for TItle I in 2008.

(63) Compare the statement on balance here with the far more outrageous one in the 2004 application.

(64) This recurrent rebuttal to efficacy questions makes me wonder whether Ron Wyden and Russ Feingold were already pushing that issue—we know that Wyden and Udall spent much of 2011 doing so.

> the measure of efficacy required to make a search “reasonable” is not a numerically demanding success rate for the search.

(65) Hey! THat redaction after “chaining” that disappeared for a while in 2009 is back, suggesting they’re planning more than simple chaining.

(70) They call 2-hop connection a “direct contact” with an identifier.

(71) Actually don’t know if “compliance report” is same thing as E2E report.

(72) THey pretend PRTT doesn’t regulate use normally.

(72) They claim the applications imposed controls, not the orders, maintaining structure that they’re the ones imposing minimization.

(72) Court has asserted, the Government has supported that assertion

(73) This is where the government claims the Court has authority to query everything.

(73) It relies on "known and extended absence provision" of FBI minimization (the logging language reminds me of the changes made in 2008, per Moalin).

(74) Govt uses language prohibiting intentional violations in criminal statutes to say that bc this wasn't intentional they should be able to access the data good faith. Which of course pretends it wasn't intentional.

S. **Declaration of General Keith B. Alexander, U.S. Army, Director, NSA, in Support of Pen Register/Trap and Trace Application**, T. **Exhibit D in Support of Pen Register/Trap and Trace Application**. U. **First Letter in Response to FISC Questions Concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**: V. **Second Letter in Response to FISC Questions concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**, W. **Third Letter in Response to FISC Questions Concerning NSA Bulk Metadata Collection Using Pen Register/Trap and Trace Devices**.

F. **FISC Primary Order**. July 2010:

(4) There seems much more emphasis on the assistance of providers; this language parallels what's in USAF.

(10) Bates switched the "will" language back to "shall" here. They also took out the ODNI language.

(12) Here's the language permitted them to access the data; it seems like it would amount to virtually all of it.

G. **FISC Memorandum Opinion Granting in Part and Denying in Part Application to Reinitiate, in Expanded Form, Pen Register/Trap and Trace Authorization**,

(8) It's interesting that they relied on a Leiter statement from a previous docket; the US approach to AQAP changed in the interim.

(11) The footnote likely admits that this application would be drawing on far more communications.

(11) Director of NSA has informed me that at no time did NSA collect any category of information … other than the [redacted] categories of meta data." "This assurance turned out to be untrue.""There is not the physical possibility of our having [collected content]

(17) Was 1000 analysts displayed in the compliance docs?

(19) The delegated approval and not for CT purpose may not be declass in other docs

(20) Overcollection was discovered by OGC

(21) Still interested in Bates' comment abt why it was allowed to continue? Did NSA delay in telling Bates?

(22) "the extraordinary fact that NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."

(23) The government did run emergency queries on at least several subjects and reported those to the court

(29) Footnote 30 modifies the redacted sentence(s). It shows inconsistent judgments on whether the government can record the "contents" of PRTT.

(35) Some of what they're discussing (which is redacted later) is logging into an account and/or processing or transmitting an email or IM communication. That counts as signaling to Bates.

(72) 11-24 fold increase in volume.

(80) This should make this not a PRTT.

> At this pre-collection stage, it is uncertain to which facilities PR/TT devices will be attached or applied during the pendency of the initial order. … For this reason, and because the Court is satisfied that other specifications in the order will adequately demarcate the scope of authorized collection, the Court will issue an order that does not identify persons pursuant to Section 1842(d)(2)(A)(ii). However, once this surveillance is implemented, the government's state of knowledge may well change. Accordingly, the Court expects the government in any future application to identify persons (as described in Section 1842(d)(2)(A)(ii)) who are know to the government for any facility that the government knows will be subjected to PR/TT surveillance during the period covered by the requested order.

(86) Apparently there's a think (data mining?) that they only do to the corporate store.

(108) "The government's descriptions of the overcollected information make clear that the information concerns the identity of the parties, the existence of the communications, or both.

July to August 2010: First of clarifying letters on dragnet order. FF: Government's First Letter to Judge Bates to Confirm Understanding of Issues Relating to the FISC's Authorization to Collect Metadata.

August 2010: Second clarifying letter on dragnet order. GG: **Government's Second Letter to Judge Bates to Confirm Understanding of Issues Relating to the FISC's Authorization to Collect Metadata**:

These both just ask for clarification of Bates' opinion on 5 issues. But it shows there was at

least a several week delay in implementing the new collection.

LEAHY FREEDOM ACT EXEMPTS FBI FROM COUNTING ITS BACK DOOR SEARCHES

As I said in my post last night, Pat Leahy's version of USA Freedom Act is a significant improvement over USA Freedumber, the watered down House version. But it includes language that no one I've met has been able to explain. I believe it may permit the NSA to have its immunized telecom providers contact chain on (at least) location, and possibly worse. Thus, it may well be everyone applauding the bill — including privacy NGOs — are applauding increased use of techniques like location spying even as judges around the country are deeming such spying unconstitutional. I strongly believe this bill may expand the universe of US persons who will be thrown into the corporate store indefinitely, to be subjected to the full brunt of NSA's analytical might.

But that's not the part of the bill that disturbs me the most. It's this language:

> '(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.

The language refers, in part, to requirements that the government report to Congress:

> (B) the total number of orders issued pursuant to section 702 and a good faith estimate of—
>
> (iv) the number of search terms that included information concerning a United States person that were used to query any database of the contents of electronic communications or wire communications obtained through the use of an order issued pursuant to section 702; and
>
> (v) the number of search queries initiated by an officer, employee, or agent of the United States whose search terms included information concerning a United States person in any database of noncontents information relating to electronic communications or wire communications that were obtained through the use of an order issued pursuant to section 702;

These are back door searches on US person identifiers of Section 702 collected data — both content (iv) and metadata (v).

In other words, after having required the government to report how many back door searches of US person data it conducts, the bill then exempts the FBI.

The FBI — the one agency whose use of such data can actually result in a prosecution of the US person in question.

We already know the government has not provided all defendants caught using 702 data notice. And yet, having recognized the need to start counting how many Americans get caught in back door searches, Patrick Leahy has decided to exempt the agency that uses back door searches the most.

And if they're not giving defendants notice (and they're not), then this is an illegal use of Section 702.

There is no reason to exempt the FBI for this. On the contrary, if we're going to count back door searches on US persons, the first place we should start counting is at FBI, where it likely matters most. But the Chair of the Senate Judiciary Committee has decided it's a good idea to exempt precisely those back door searches from reporting requirements.

IMPROVED USA FREEDOM RETAINS "CONNECTION" CHAINING AND "FOREIGN INTELLIGENCE" RETENTION

Thanks to this NYT editorial, everyone is talking about Patrick Leahy's version of USA Freedom, which he will introduce tomorrow.

Given what I've heard, my impression is the editorial is correct that Leahy's bill is a significant improvement off of USA Freedumber.

That's not saying much.

It tightens the definition for Specific Selection Term significantly (though there may still be limited cause for concern).

It improves the FISA Advocate (but not necessarily enough that it would be meaningful).

It improves transparency (but there's one aspect of "improved" transparency that actually disturbs me significantly).

It pretends to fix concerns I had about the PRTT minimization, but I don't think it succeeds.

Still, an improvement off of the USA Freedumber.

I'm not convinced that makes it an acceptable improvement off of the status quo (especially the status quo requiring court approval for each seed). That's because — from what I've heard — Leahy's bill retains the language from USA Freedumber on contact chaining, which reads,

> (iii) provide that the Government may require the prompt production of call detail records—
>
> (I) using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii) as the basis for production; and
>
> (II) using call detail records with a direct connection to such specific selection term as the basis for production of a second set of call detail records;

Now, I have no idea what this language means, and no one I've talked to outside of the intelligence committees does either. It might just mean they will do the same contact chaining they do now, but if it does, why adopt this obscure language? It may just mean they will correlate identities, and do contact chaining off all the burner phones their algorithms say are the same people, but nothing more, but if so, isn't there clearer language to indicate that (and limit it to that)?

But we know in the equivalent program for DEA — Hemisphere — the government uses location to chain people. So to argue this doesn't include location chaining, you'd have to argue that NSA is satisfied with less than DEA gets and explain why the language of this bill specifically prohibits it. (The bill — as USA Freedumber before it did — requires NSA to use Call Detail Records at each step; that may or may not impose

such limits.)

I remain concerned, too, that such obscure language would permit the contact chaining on phone books and calendars, both things we know NSA obtains overseas, both things NSA might have access to through their newly immunized telecom partners.

In addition, Leahy's bill keeps USA Freedumber's retention language tied to Foreign Intelligence purpose, allowing the NSA to keep all records that might have a foreign intelligence purpose.

Why, after having read PCLOB's 702 report stating that, "when an NSA analyst recognizes that [a communication] involves a U.S. person and determines that it clearly is not relevant to foreign intelligence or evidence of a crime," destruction of it, which is required by the law, "rarely happens," would anyone applaud a Section 215 bill that effectively expands retention using that very same utterly meaningless "foreign intelligence" language? And with it may expand the permitted *dissemination* of such data?

The bill is definitely an improvement over USA Freedumber. But until someone explains what that connection chaining language does — and includes limiting language to make sure that's all it will ever do — I have no way of knowing whether Leahy's bill is better than the status quo. As it is, however, it is certainly conceivable Leahy's bill will result in more innocent Americans ending up in the corporate store.

(I may have two more *new* concerns about Leahy's bill, but I'll hold those until I see what precise language the bill uses for them.)

ALL THESE MUSLIM ORGANIZATIONS HAVE PROBABLY BEEN ASSOCIATIONALLY MAPPED

The Intercept has published their long-awaited story profiling a number of Muslim-American leaders who have been targeted by the FBI and NSA. It shows that:

- American Muslim Council consultant Faisal Gill was surveilled from April 17, 2006 to February 8, 2008
- al-Haramain lawyer Asim Ghafoor was surveilled under FISA (after having been surveilled illegally) starting March 9, 2005; that surveillance was sustained past March 27, 2008
- American Muslim Alliance founder Agha Saeed was surveilled starting June 27, 2007; that surveillance was sustained past May 23, 2008
- CAIR founder Nihad Awad was surveilled from July 17, 2006 to February 1, 2008
- American Iranian Council founder Hooshang Amirahmadi was surveilled from August 17, 2006 to May 16, 2008

In other words, the leaders of a number of

different Muslim civil society organizations were wiretapped for years under a program that should require a judge agreeing they represent agents of a foreign power.

But they probably weren't just wiretapped. They probably were also used as seeds for the phone and Internet dragnets, resulting in the associational mapping of their organizations' entire structure.

On August 18, 2006, the phone dragnet primary order added language deeming "telephone numbers that are currently the subject of FISA authorized electronic surveillance … approved for meta data querying without approval of an NSA official due to the FISA authorization."

Given the way the phone and Internet dragnet programs parallel each other (and indeed, intersect in federated queries starting at least by 2008), a similar authorization was almost certainly included in the Internet dragnet at least by 2006.

That means as soon as these men were approved for surveillance by FISA, the NSA also had the authority to run 3-degree contact chaining on their email and phone numbers. All their contacts, all their contacts' contacts, and all their contacts' contacts' contacts would have been collected and dumped into the corporate store for further NSA analysis.

Not only that, but all these men were surveilled during the period (which continued until 2009) when the NSA was running automated queries on people and their contacts, to track day-to-day communications of RAS-approved identifiers.

So it is probably reasonable to assume that, at least for the period during which these men were under FISA-authorized surveillance, the NSA has an associational map of their organizations and their affiliates.

Which is why I find it interesting that DOJ refused to comment on this story, but told other reporters that FBI had never had a FISA warrant

for CAIR founder Nihad Awad specifically.

> The Justice Department did not respond to repeated requests for comment on this story, or for clarification about why the five men's email addresses appear on the list. But in the weeks before the story was published, *The Intercept* learned that officials from the department were reaching out to Muslim-American leaders across the country to warn them that the piece would contain errors and misrepresentations, even though it had not yet been written.
>
> Prior to publication, current and former government officials who knew about the story in advance also told another news outlet that no FISA warrant had been obtained against Awad during the period cited. When *The Intercept* delayed publication to investigate further, the NSA and the Office of the Director of National Intelligence refused to confirm or deny the claim, or to address why any of the men's names appear on the FISA spreadsheet.

Awad's organization, CAIR, is a named plaintiff in the EFF's suit challenging the phone dragnet. They are suing about the constitutionality of a program that – the EFF suit also happens to allege – illegally mapped out associational relations that should be protected by the Constitution.

CAIR now has very good reason to believe their allegations in the suit – that all their relationships have been mapped – are absolutely correct.

Update: EFF released this statement on the Intercept story, reading, in part,

> > Surveillance based on First Amendment-protected activity was a stain on our nation then and

> > continues to be today. These disclosures yet again demonstrate the need for ongoing public attention to the government's activities to ensure that its surveillance stays within the bounds of law and the Constitution. And they once again demonstrate the need for immediate and comprehensive surveillance law reform.
>
> We look forward to continuing to represent CAIR in fighting for its rights, as well as the rights of all citizens, to be free from unconstitutional government surveillance.

EFF represents CAIR Foundation and two of its regional affiliates, CAIR-California and CAIR-Ohio, in a case challenging the NSA's mass collection of Americans' call records. More information about that case is available at: *First Unitarian Church of Los Angeles v. NSA*.

THE BLACK HOLES IN USA FREEDUMBER'S INSPECTOR GENERAL REPORTS

I'm still working on understanding all the crud that is included in the USA Freedumber Act. And for the first time, I have looked really closely at the language on Inspector General Reports, which effectively modifies Section 106 of the 2005 PATRIOT Act Reauthorization. Not

only does the language add a DOJ IG Report roughly parallel to the ones mandated for the years through 2006 for 2012 through 2014, but it adds an Intelligence Community IG Report for those 3 years.

I've long noted that that seems to leave 2010 and 2011 unexamined. That might be covered in the IG report Pat Leahy requested of the Intelligence Committee IG, Charles McCullough, though the dates are different and McCullough said he didn't really have the time. So 2010 and 2011 may or may not currently being reviewed; they're not required to be by the bill, however.

But upon closer review I'm just as interested in some holes the two reports will likely have, in combination.

What I realized when I reviewed the actual language, below, is that USA Freedumber is exploiting the fact that Section 215 was originally written exclusively for the FBI, even if the NSA and CIA and probably a bunch of other agencies are using it too (they're doing this with minimization procedures elsewhere in the bill, too). Thus, they can leave language that applies specifically to FBI, and pretend that it applies to other agencies.

In practice, that leaves the DOJ IG to investigate general things about Section 215 use, including:

- any noteworthy facts or circumstances relating to orders under such section, including any improper or illegal use of the authority provided under such section; and
- the categories of records obtained and the importance of the information acquired to the intelligence activities of the Federal Bureau of Investigation or any other Department or

> agency of the Federal Government;

So long as FBI retains a role in the application process, it will have access to and can review the categories of records obtained, which is critical because this is one of the ways Congress will learn what those categories are.

But only the DOJ IG assesses whether Section 215 is adhering to law (as opposed to protecting Americanas' constitutional rights). At one level, I'd *much* rather have DOJ IG perform this review, because we've never seen anything out of the IC IG resembling real oversight. Plus, under Glenn Fine, DOJ's IG did point to real legal problems with the dragnet (which DOJ largely refused to fix, but which may have led to addition FISC opinions on those subjects). But I have questions whether DOJ's IG would get enough visibility into what NSA and CIA and other agencies are doing with this data to perform a real review of the legality of it.

Then there are some somewhat parallel things both DOJ's and IC's IG would review, including:

- the importance (IC IG) or effectiveness (DOJ IG) of Section 215
- the manner in which that information was collected, retained, analyzed, and disseminated by the intelligence community;
- the minimization procedures used by elements of the intelligence community under such title and whether the minimization procedures adequately protect the constitutional rights of United States persons; and
- any minimization procedures proposed by an element of the intelligence community under such title that were modified or denied by the FISC

These are all well and good, and there's the

possibility that an IC IG review of how NSA analyzes and disseminates Section 215 data would find any of the most concerning potential practices.

I find the last two things DOJ's IG would review at FBI but not even at DEA (if DEA uses Section 215), and which the IC IG would not review at all, the most telling.

- whether, and how often, the Federal Bureau of Investigation used information acquired pursuant to an order under section 501 of such Act to produce an analytical intelligence product for distribution within the Federal Bureau of Investigation, to the intelligence community or to other Federal, State, local, or tribal government Departments, agencies, or instrumentalities; and
- whether, and how often, the Federal Bureau of Investigation provided such information to law enforcement authorities for use in criminal proceedings

That is, the DOJ IG reports on how often the FBI uses Section 215 for finished intelligence products and how often it serves supports criminal proceedings. But it doesn't track how often NSA uses Section 215 for finished intelligence products, nor does it track how often NSA uses Section 215 to investigate an American further.

The latter fact – that NSA isn't counting how many Americans its targets because of Section 215 derived information – is not all that surprising. NSA has worked hard to obscure how many Americans have been sucked up in its analytical maw. Still, if we were serious about providing some transparency to the corporate store – where anyone 2 or 3 degrees from a RAS approved selector can get dumped and subjected to all of NSA's analytical tradecraft forever – we'd require the IC IG to count this number, too.

And the fact that no one asks NSA and CIA how many finished intelligence reports they're generating out of Section 215 is problematic both because it doesn't identify how often NSA and CIA are sharing intelligence with FBI or National Counterterrorism Center or other agencies like DEA (which was one of the big problems with both the phone and Internet dragnet in 2009-10). But it also makes it harder for Congress to get a real understanding of how effective these tools are.

You can't judge the efficacy of something you don't measure.

To understand how important this is, consider the discussions about the phone dragnet we've had since last year. Everything has been measured in terms of reporting to FBI, which not only doesn't disclose how many people are stuck in NSA's maw, but to outsiders made the program look totally useless. We still don't know precisely how the government is using the phone dragnet, because the data they've shared to describe its efficacy is probably not the most significant way it is used.

It seems the intelligence community would like to keep it that way.

SEC. 106A. AUDIT ON ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES.

(a) Audit.—The Inspector General of the

Department of Justice shall perform a comprehensive audit of the effectiveness and use, including any improper or illegal use, of the investigative authority provided to the Federal Bureau of Investigation under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.).

(b) Requirements.—The audit required under subsection (a) shall include—

(1) an examination of each instance in which the Attorney General, any other officer, employee, or agent of the Department of Justice, the Director of the Federal Bureau of Investigation, or a designee of the Director, submitted an application to the Foreign Intelligence Surveillance Court (as such term is defined in section 301(3) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1821(3))) for an order under section 501 of such Act during the calendar years of 2002 through 2006 *and*
calendar years 2012 through 2014, including—

(A) whether the Federal Bureau of Investigation requested that the Department of Justice submit an application and the request was not submitted to the court (including an examination of the basis for not submitting the application);

(B) whether the court granted, modified, or denied the application (including an examination of the basis for any modification or denial);

[two paragraphs assessing bureaucratic impediments to getting Section 215 orders approved in DOJ taken out]

(2) any noteworthy facts or circumstances relating to orders under such section, including any improper or illegal use of the authority provided under such section; and

(3) an examination of the effectiveness of such section as an investigative tool, including—

(A) the categories of records obtained and the importance of the information acquired to the

intelligence activities of the Federal Bureau of Investigation or any other Department or agency of the Federal Government;

(B) the manner in which such information is collected, retained, analyzed, and disseminated by the Federal Bureau of Investigation, including any direct access to such information (such as access to "raw data") provided to any other Department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;

(C) *with respect to calendar years 2012 through 2014, an examination of the minimization procedures used in relation to orders under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) and whether the minimization procedures adequately protect the constitutional rights of United States persons;*

(D) whether, and how often, the Federal Bureau of Investigation utilized information acquired pursuant to an order under section 501 of such Act to produce an analytical intelligence product for distribution within the Federal Bureau of Investigation, to the intelligence community *[language on National Security Act definition of intelligence community struck]*, or to other Federal, State, local, or tribal government Departments, agencies, or instrumentalities; and

(E) whether, and how often, the Federal Bureau of Investigation provided such information to law enforcement authorities for use in criminal proceedings.

(c) Submission Dates.— (1) Prior years.—Not later than one year after the date of the enactment of this Act, or upon completion of the audit under this section for calendar years 2002, 2003, and 2004, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and

the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2002, 2003, and 2004.

(2) Calendar years 2005 and 2006.—Not later than December 31, 2007, or upon completion of the audit under this section for calendar years 2005 and 2006, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2005 and 2006.

(3) CALENDAR YEARS 2012 THROUGH 2014.—Not later than December 31, 2015, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the audit conducted under subsection (a) for calendar years 2012 through 2014.

(d) INTELLIGENCE ASSESSMENT.—

(1) IN GENERAL.—For the period beginning on January 1, 2012, and ending on December 31, 2014, the Inspector General of the Intelligence Community shall assess—

(A) the importance of the information acquired under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) to the activities of the intelligence community

(B) the manner in which that information was collected, retained, analyzed, and disseminated by the intelligence community;

(C) the minimization procedures used by elements of the intelligence community under such title

and whether the minimization procedures adequately protect the constitutional rights of United States persons; and

(D) any minimization procedures proposed by an element of the intelligence community under such title that were modified or denied by the court established under section 103(a) of such Act (50 U.S.C. 1803(a)).

(2) SUBMISSION DATE FOR ASSESSMENT.—

Not later than 180 days after the date on which the Inspector General of the Department of Justice submits the report required under subsection (c)(3), the Inspector General of the Intelligence Community shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2012 through 2014.

(e) Prior Notice to Attorney General and Director of National Intelligence; Comments.—

(1) <<NOTE: Deadline. Reports.>> Notice.—Not less than 30 days before the submission of *any report under subsection (c) or (d), Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, and any Inspector General of an element of the intelligence community that prepares a report to assist the Inspector General of the Department of Justice or the Inspector General of the Intelligence Community in complying with the requirements of this section* shall provide such report to the Attorney General and the Director of National Intelligence.

(2) Comments.—The Attorney General or the Director of National Intelligence may provide comments to be included in *any report submitted under subsection (c) or (d)* as the Attorney General or the Director of National Intelligence may consider necessary.

(f) Unclassified Form.—*Each report submitted under subsection (c)* and any comments included under *subsection (e)(2)* shall be in unclassified form, but may include a classified annex.

(g) DEFINITIONS.—In this section:

(1) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) UNITED STATES PERSON.—The term 'United States person' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

FOUR REASONS USA FREEDUMBER IS WORSE THAN THE STATUS QUO

In the post-HR 3361 passage press conference yesterday, Jerry Nadler suggested the only reason civil libertarians oppose the bill is because it does not go far enough.

That is, at least in my case, false.

While I have concerns about unintended consequences of outsourcing holding the call data to the telecoms (see my skepticism that it ends bulk collection here and my concerns about high volume numbers here), there are a number of ways that USA Freedumber is worse than the status quo.

These are:

- The move to telecoms codifies changes in the chaining process that will almost certainly expand the

universe of data being analyzed
- In three ways, the bill permits phone chaining for purposes outside of counterterrorism
- The bill weakens minimization procedures on upstream collection imposed by John Bates, making it easier for the government to collect domestic content domestically
- The bill guts the current controls on Pen Register authority, making it likely the government will resume its Internet dragnet

The NSA in your smart phone: Freedumber codifies changes to the chaining process

As I have described, the language in USA Freedumber makes it explicit that the government and its telecom partners can chain on *connections* as well as actual phone call contacts. While the new automatic search process approved by the FISA Court in 2012 included such chaining, by passing this bill Congress endorses this approach. Moreover, the government has never been able to start running such automatic queries; it appears they have to outsource to the telecoms to be able to do so (probably in part to make legal and technical use of location data). Thus, moving the phone chaining to the telecoms expands on the kinds of chaining that will be done with calls.

We don't know all that that entails. At a minimum (and, assuming the standard of proof is rigorous, uncontroversially) the move will allow the government to track burner phones, the new cell phones targets adopt after getting rid of

an old one.

It also surely involves location mapping. I say that, in part, because if they weren't going to use location data, they wouldn't have had to move to the telecoms. In addition, AT&T's Hemisphere program uses location data, and it would be unrealistic to assume this program wouldn't include at least all of what Hemisphere already does.

But beyond those two functions, your guess is as good as mine. While the chaining must produce a Call Detail Record at the interim step (which limits how far away from actual phone calls the analysis can get), it is at least conceivable the chaining could include any of a number of kinds of data available to the telecoms from smart phones, including things like calendars, address books, and email.

The fact that the telecoms and subsidiary contractors get immunity and compensation makes it more likely that this new chaining will be expansive, because natural sources of friction on telecom cooperation will have been removed.

Freedumber provides three ways for NSA to use the phone dragnet for purposes besides counterterrorism

As far as we know, the current dragnet may only be used for actual terrorist targets and Iran. But USA Freedumber would permit the government to use the phone dragnet to collect other data by:

- Requiring only that selection terms be associated with a foreign power
- Permitting the retention of data for foreign intelligence, not just counterterrorism, purposes
- Allowing the use of

emergency queries for non-terrorism uses

Freedumber permits searches on selection terms associated with foreign powers

On its face, USA Freedumber preserves this counterterrorism focus, requiring any records obtained to be "relevant to" an international terrorist investigation. Unfortunately, we now know that FISC has already blown up the meaning of "relevant to," making all data effectively relevant.

The judicial approval of the specific selection term, however — the court review that should be an improvement over the status quo — is not that tie to terrorism, but evidence that the selection term is a foreign power or agent thereof.

Thus, the government could cite narcoterrorism, and use the chaining program to investigate Mexican drug cartels. The government could raise concerns that al Qaeda wants to hack our networks, and use chaining to investigate hackers with foreign ties. The government could allege Venezuela supports terrorism and investigate Venezuelan government sympathizers.

There are a whole range of scenarios in which the government could use this chaining program for purposes other than counterterrorism.

Freedumber permits the retention of any data that serves a foreign intelligence purpose

And once it gets that data, the government can keep it, so long as it claims (to itself, with uncertain oversight from the FISC) that the data has a foreign intelligence purpose.

At one level, this is a distinction without a difference from the language that USA Freedumb had used, which required the NSA to destroy the data after five years unless it was relevant to a terrorism investigation (which all data turned over to NSA would be, by definition). But the change in language serves as legislative

approval that the use of the data received via this program can be used for other purposes.

That will likely have an impact on minimization procedures. Currently, the NSA needs a foreign intelligence purpose to access the corporate store, but can only disseminate data from it for counterterrorism purposes. I would imagine the changed language of the bill will lead the government to successfully argue that the minimization procedures permit the dissemination of US person data so long as it meets only this flimsy foreign intelligence purpose. In other words, US person data collected in chaining would be circulating around the government more freely.

Freedumber's emergency queries do not require any tie to terrorism

As I noted, the revisions USA Freedumber made to USA Freedumb explicitly removed a requirement that emergency queries be tied to a terrorism investigation.

> (A) reasonably determines that an emergency situation requires the production of tangible things to ~~obtain information for an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism~~ before an order authorizing such production can with due diligence be obtained;

That's particularly troublesome, because even if the FISC rules the emergency claim (certified by the Attorney General) was not legally valid after the fact, not only does the government *not* have to get rid of that data, but the Attorney General (the one who originally authorized its collection) is the one in charge of making sure it doesn't get used in a trial or similar proceeding.

In short, these three changes together permit the government to use the phone dragnet for a

lot more uses than they currently can.

Freedumber invites the expansion of upstream collection

When John Bates declared aspects of upstream collection to be unconstitutional in 2011, he used the threat of referrals under 50 USC 1809(a) to require the government to provide additional protection both to entirely domestic communications that contained a specific selector, and to get rid of domestic communications that did not contain that specific selector at all. The government objected (and considered appealing), claiming that because it hadn't really intended to collect this data, it should be able to keep it and use it. But ultimately, that threat (especially threats tied to the government's use of this data for ongoing FISA orders) led the government to capitulate.

The changes in Freedumber basically allow the government to adopt its old "intentional" claim, reversing Bates' restrictions. That's because they only have to extend protection to domestic communications if they're from an identifiable US person, rather than from a US person location (NSA has claimed they have a hard time identifying a lot of this data). And, more troubling, they only have to minimize such communications if they recognize them as such at the moment they collect it. Finally, they only have to do so "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information," basically providing the government a giant loophole not even to do that.

Effectively, then, this language on upstream searches will permit the government to use upstream searches to collect and keep domestic communications because they need to collect foreign intelligence.

Under Freedumber, the government will almost certainly resume the Internet dragnet

In a very similar but even more alarming

fashion, USA Freedumber also reverses John Bates' 2010 efforts to shut down the illegal Internet dragnet.

As I explained in this post, from the very start of the FISC-sanctioned dragnet, the government claimed that the Pen Register statute permitted the judge only a very circumscribed role rubber stamping applications. Effectively, revised language in USA Freedumber would codify that stance in law.

Of particular concern, USA Freedumber replaced USA Freedom Act's language codifying minimization procedures (and FISC's ability to review compliance with them) with language requiring the Attorney General to develop privacy procedures. The application of those procedures, like the minimization procedures for upstream collection, will be secondary to "the need to protect national security."

In addition, USA Freedumber exempts PRTT from some of the reporting requirements, making the detailed practices of PRTT less visible to Congress.

From what we know about the Internet dragnet, Colleen Kollar-Kotelly imposed limits on the Internet dragnet, which the NSA violated — and lied about — right away. As part of the reviews done in 2009, FISC discovered NSA was still and always had been violating those restrictions. Internet dragnet collection may have been halted from 2009 to 2010, but in 2010, Bates reimposed limits (it's not clear if these were the same ones imposed by Kollar-Kotelly). The NSA "shut down" the program a year or so after Bates imposed those limits (though there are reasons to doubt it got shut down, rather than just moved), apparently because it just wasn't all that useful once they had to follow the rules. Bates used two levers to be able to impose these requirements: the assumption he could impose minimization procedures, and that threat of using 50 USC 1809(a) to limit the use of illegally collected data going forward.

By explicitly denying FISC the authority to impose minimization procedures, USA Freedumber effectively takes away all the leverage FISC used to ensure that the Internet dragnet stopped being domestic content acquisition program.

The only question is whether the requirement that all production begin from a "specific selection term" would prevent the resumption of the Internet dragnet. I don't think it would. That's because the entire program always was based on specific selection terms — tied to telecom circuits, based on the claim those circuits carried a higher percentage of terrorism traffic than other circuits. By resuming the Internet dragnet on those circuits (but not all of them, thereby using a discriminator), NSA can claim it is not engaging in bulk collection, and still get away with resuming the Internet dragnet.

And the best part? The telecoms would now have immunity to help NSA collect domestic content in the US.

Just before the vote yesterday, the tech companies withdrew their support for the bill, saying that "The latest draft opens up an unacceptable loophole that could enable the bulk collection of Internet users' data." They appear to believe the loophole derives from the wide open definition of "specific selection term." But if I'm right about these last two changes, then the loophole is salted throughout the bill. And it would put the telecoms back in the business of stealing Internet content (to the extent that it is accessible) as it passed their backbone. If I'm right about that — and if the Internet companies realize it — then we have a hope of preventing this shitty, worse than status quo bill from becoming law.

But whether we will nor not remains to be seen.

Update: Given the way I believe US Freedumber guts leverage that John Bates exercised over NSA, I find this comment from him — from 3 weeks ago — striking.

> Bates also sounded dubious about proposals—like Obama's—to have phone companies store call metadata instead of the government. The judge said he's more confident that "compliance" issues can be addressed at a government agency like the NSA than at private companies.
>
> "My experience tells me that I can hold the NSA's feet to the fire a lot easier than I can hold Google or Verizon's feet to the fire," Bates said. He noted that he has considerable leverage over the NSA, because they want to keep running the program and need the court's permission to do so. On the other hand, "the private companies want the program cut off," so would have less incentive to address problems, he added.

WILL THE DRAGNET REFORM CRIMINALIZE ORDERING PIZZA?

There are two major problems with the phone dragnet, as it currently exists.

First, the government has a database of all the phone-based relationships in the United States, one they currently (as far as we know) do not abuse, but one that is ripe for unbelievable abuse.

But there is current abuse going on. The dragnet takes completely innocent people who are three (now two) degrees of separation from someone subjected to a digital stop-and-frisk, a very low standard, and puts them (by dint of at least one communication with someone who communicated with someone who might be suspicious) into the NSA's analytical maw. Permanently. Those people

can have their multiple IDs connected, including any online searches NSA happened to injest, they can be subjected to data mining, by dint of those conversations, they apparently can even have the content of their communications accessed without a warrant, they might even be targeted to become informants using the data available to NSA.

This may well be the digital equivalent of J Edgar Hoover's subversives list, a collection of people who will always be subject to heightened scrutiny, including unbelievably invasive digital analysis, because of a three degree association years in the past.

According to PCLOB's estimate, as many as 120 million people may have been — may still be! — subjected for this treatment.

Discussions of whether the House Judiciary and Intelligence Committee bills "reforming" the dragnet really fix it have almost entirely ignored this second abuse, the innocent people who will be subjected to the "full range of NSA's analytical tradecraft" merely because of a potentially completely innocent association.

There are things that should be done — whether in the current dragnet or the "reformed" one — to mitigate this abuse. Those data ought to age off, which they currently don't (and won't, under the new program, as currently described). That analysis ought to be subject to audits, which they're not currently. The FISC ought to get some sense of what happens in this corporate store, which it's not clear it currently has. Criminal defendants ought to have some visibility into whether their prosecutions stemmed from such analysis.

But there are also things — as Congress crafts a dragnet replacement — that can affect the sheer number of new people who will be thrown into the corporate store, into NSA's analytical pool. And those things have a lot to do with how this new scheme deals with what is called "data integrity."

As I have written repeatedly, the number of results NSA (or the telecoms, under the new system) will get under a particular query depends on how many noisy numbers — things like telemarketers, voice mail numbers, and pizza joints — remain in the collection. As Jonathan Mayer showed, even in his 300 person dataset that included just 2 people who had ever called each other, 17% were connected at the second hop through T-Mobile's voice mail number.

> In spite of the fact that just 2 of its participants had called each other, the fact that so many people had called T-Mobile'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.

We know NSA currently does significant work to pull those noisy numbers via a "data integrity" process both before new data is used for contact chaining and as new numbers are identified as "high volume numbers." While we don't get to assess the efficacy of that process, it can make the difference between hundreds of millions of Americans getting thrown into the NSA's analytical pool, or just tens of thousands. But as the contact-chaining process gets outsourced to the telecoms, the question becomes more pressing.

As I see it, there are three possible ways this function might be done going forward:

1. The telecoms do an initial sort of high volume numbers, taking out voice mail box and telemarketer calls, then pass the data onto NSA, which does a secondary sort to pull out things like pizza joints (which NSA might want to keep in the data set, but suppress in contact chaining until they have evidence a pizza joint might be a key hub in a terrorist attack). This plays to existing telecom strengths (most likely do similar analysis on their own use of the data now), but doesn't require they make what are analytical intelligence decisions. Even though this is likely the best solution, it still means many completely

innocent Americans may be subject to NSA's analysis because they ordered pizza.

2. The telecom does all the data integrity analysis, identifying all the high volume numbers. This would result in the fewest number (but still intolerably too many) of innocent Americans being dumped into NSA's pot. But it would also turn the telecoms into an arm of US intelligence (well, even more than they already are!), because they'd be in the position of making analytical judgments about what data is useful for NSA's intelligence purposes. Which may be one of the reasons the telecoms seem to be demanding immunity, again.
3. NSA does the data integrity analysis at the telecoms, as seems to be envisioned by the HPSCI bill. This might achieve the current status quo, borrowing on 8 years of experience to strike the right balance. But it would also present the intolerable condition of NSA employees or contractors accessing and analyzing the raw data of private communications

> providers at the providers' locales.

When I asked a White House Senior Administration Official back in March how this function would be done, she had no answer (though it sounded like the government might ask the telecoms to do all of this).

> Under the President's proposal, the government would seek court orders compelling the companies to provide technical assistance to ensure the information can be queried, to run the queries, and to give the records back to the government in a usable format and on a timely basis. As additional questions arise with respect to the proposal, we look forward to working through them with Congress and relevant stakeholders to craft legislation that embodies the key attributes of this new approach.

That is, the White House is leaving it to Congress to deal with this, but thus far this is the extent of the discussion of its resolution in the two bills:

HPSCI

> [T]he Attorney General and the Director of National Intelligence may direct, in writing, an electronic communications service provider to –
>
> (A) immediately provide the Government with records, whether existing or created in the future, in the format specified by the Government and in a manner that will protect the secrecy of the acquisition;
>
> [snip]
>
> The Government may provide any information, facilities, or assistance necessary to aid the electronic

> communications service provider in complying with a directive issued pursuant to paragraph (1).

HJC

> [Orders will] direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production;

While there are hints of this question in this language (and the SAO I asked about it seemed aware the issue existed), no one is explicitly discussing who will ensure that hundreds of millions of completely innocent Americans aren't sucked up because they checked their voice mail or ordered a pizza.

And with language like this (from the HJC bill), it leaves open the possibility the numbers of innocent people who have their data handed to NSA — because they are, by definition, relevant to an investigation — will be kept and analyzed forever.

> (v) direct the Government to destroy all call detail records produced under the order not later than 5 years after the date of the production of such records, except for records that are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism.

There are many things that need to be fixed in

these bills – including the language on how long the NSA can keep and analyze potentially innocent data handed over because of query noise.

But Congress needs to be cognizant that this very basic question – who cleans up the data – will have a potentially enormous impact on how abusive this program will be going forward. Because if they're not, it is easily conceivable that **more** completely innocent people will be subjected to NSA's analytical might than currently happens under the dragnet.

Update: Interesting. HPSCI just released a managers amendment that adds language on providing facilities:

> '(ii) information, facilities, or assistance necessary to provide the records described in clause (i);

That seems to be a change from the government providing assistance, above.

"FACTS MATTER" SAID NSA YAY-MAN MICHAEL HAYDEN WHO TOLD SERIAL LIES ABOUT THE PHONE DRAGNET

I'm not sure if you saw last night's Munk Debate pitting Glenn Greenwald and Alexis Ohanian against Michael Hayden and Alan Dershowitz. I did a whole slew of fact checking and mockery on twitter last night.

But I wanted to pay particular attention to a string of false claims Hayden made about the phone dragnet program.

First, my hobbyhorse, he claimed the database can only be used for terror. (After 1:08)

> If this program — and here we're talking about the metadata program — which is about terrorism, because the only reason you can use the metadata is to stop terrorism. No other purpose.

Actually, terrorism and … Iranian "terrorism." It's unclear when or why or how Iran got included in database access (though it is considered a state sponsor of terror). But according to Dianne Feinstein and Keith Alexander, analysts can also access the database for Iran-related information. Now, maybe they can only access the Iran data if they claim terror. But that's a very different thing than claiming a tie to al Qaeda.

The real doozies come later (my transcription; after 1:20:40; I've numbered the false claims and provided the "facts matter" below).

> I started out with facts matter. So I assume on the metadata issue we're talking about the 215 program. About the phone records, alright? Because frankly, that's the only bulk metadata NSA has on American citizens. **(1)**
>
> [cross talk]
>
> Accusations fit on a bumper sticker. The truth takes longer. NSA gets from American telephone providers the billing records of American citizens. **(2)** What happens to the billing records is actually really important. I didn't make this phrase up but I'm gonna use it. They put it in a lock box, alright? They put it in a lock box at NSA. **(3)** 22 people at NSA are allowed to access that lockbox. **(4)** The only thing NSA is allowed to do with that truly gajillion record field sitting there is that when they have what's called a seed number, a seed number about which they have

> reasonable articulable suspicion that that seed number is affiliated with al Qaeda – you roll up a safe house in Yay-Man, he's got pocket litter, that says here's his al Qaeda membership card, he's got a phone you've never seen before. Gee, I wonder how this phone might be associated with any threats in the United States. **(5)** So, I'll be a little cartoonish about this, NSA gets to walk up to the transom and yell through the transom and say hey, anybody talk to this number I just found in Yay-Man? And then, this number, say in Buffalo, says well, yeah, I call him about every Thursday. NSA then gets to say okay Buffalo number – by the way, number, not name – Buffalo number, who did you call. At which point, by description the 215 metadata program is over. That's all NSA is allowed to do with the data. There is no data mining, there's no powerful algorithms chugging through it, trying to imagine relationships. **(6)** It's did that dirty number call someone in the United States. The last year for which NSA had full records is 2012 – I'll get the 13 numbers shortly **(7)** – but in 2012, NSA walked up to that transom and yelled "hey! anybody talk to this number?" 288 times. **(8)**

(1) Under the SPCMA authority, NSA can include US persons in contact-chaining of both phone and Internet metadata collected overseas. SPCMA has far fewer of the dissemination and subject matter limitations that the Section 215 dragnet has.

(2) NSA doesn't get the "billing records." It gets routing information, which includes a great deal of data (such as the cell phone and SIM card ID and telecom routing information) that wouldn't be included on a phone bill, even assuming a bill was itemized at all (most local

landline calls are not). It also gets the data every day, not every month, like a billing record.

(3) Starting in early January 2008, NSA made a copy of the dragnet data and "for the purposes of analytical efficiency" dumped it in with all their other metadata. That allows them to conduct "federated queries," which is contact chaining across authorities (so chains including both foreign collected EO12333 data and domestic Section 215 data). The NSA coaches its analysts to rerun queries that are replicable in EO12333 alone because of the greater dissemination that permits.

(4) The 22 number refers to the people who can approve an identifier for Reasonable Articulable Suspicion, not the people who can conduct queries. Those 22 are:

> the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate.

While we don't know how many analysts are trained on Section 215 dragnet right now, the number was 125 in August 2010.

But even those analysts are not the only people who can access the database. "Technicians" may do so too.

> Appropriately trained and authorized technical 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 terms 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 ill 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 of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes.

And this access — which requires access to the raw metadata — is not audited.

(5) Note, in the past, the government has also accessed the database with "correlated" identifiers — phone numbers and SIM cards associated with the same person. It's unclear what the current status of querying on correlated identifiers is, but that is likely the topic of one of the FISC opinions the government is withholding, and the government is withholding the opinion in question in the name of protecting an ongoing functionality.

(6) Hayden pretends there's a clear boundary to this program, but even the FISC minimization procedures for it approve the corporate store, where these query results — people 2 degrees from someone subjected to a digital stop-and-frisk — may be subjected to "the full range of [NSA's] analytic tradecraft." So when Hayden says there's no data mining and no powerful algorithms, he's lying about the data mining and powerful algorithms (and content access) that are permitted for identifiers in the corporate store.

(7) Given that DOJ has already released their numbers for FISA use in 2013, I presume it also has the number of identifiers that have been

queried.

(8) The 288 number refers to the number of identifiers queried, not the number of queries run. Given that the dragnet serves as a kind of alert system — to see who has had contracts with a certain number over time — the number of actual queries is likely significantly higher, as most of the identifiers were likely run multiple times.

THE VERIZON PUBLICITY STUNT, MOSAIC THEORY, AND COLLECTIVE FOURTH AMENDMENT RIGHTS

On Friday, I Con the Record revealed that a telecom — Ellen Nakashima confirms it was Verizon — asked the FISA Court to make sure its January 3 order authorizing the phone dragnet had considered Judge Richard Leon's December 16 decision that it was unconstitutional. On March 20, Judge Rosemary Collyer issued an opinion upholding the program.

Rosemary Collyer's plea for help

Ultimately, in an opinion that is less shitty than FISC's previous attempts to make this argument, Collyer examines the US v. Jones decision at length and holds that Smith v. Maryland remains controlling, mostly because no majority has overturned it and SCOTUS has provided no real guidance as to how one might do so. (Her analysis raises some of the nuances I laid out here.)

The section of her opinion rejecting the "mosaic theory" that argues the cumulative effect of

otherwise legal surveillance may constitute a search almost reads like a cry for help, for guidance in the face of the obvious fact that the dragnet is excessive and the precedent that says it remains legal.

> A threshold question is which standard should govern; as discussed above, the court of appeals' decision in Maynard and two concurrences in Jones suggest three different standards. See Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Mich. L. Rev. at 329. Another question is how to group Government actions in assessing whether the aggregate conduct constitutes a search.See id. For example, "[w]hich surveillance methods prompt a mosaic approach? Should courts group across surveillance methods? If so, how? Id. Still another question is how to analyze the reasonableness of mosaic searches, which "do not fit an obvious doctrinal box for determining reasonableness." Id. Courts adopting a mosaic theory would also have to determine whether, and to what extent, the exclusionary rule applies: Does it "extend over all the mosaic or only the surveillance that crossed the line to trigger a search?"
>
> [snip]
>
> Any such overhaul of Fourth Amendment law is for the Supreme Court, rather than this Court, to initiate. While the concurring opinions in Jones may signal that some or even most of the Justices are ready to revisit certain settled Fourth Amendment principles, the decision in Jones itself breaks no new ground concerning the third-party disclosure doctrine generally or Smith specifically. The concurring opinions notwithstanding, Jones simply cannot be read as inviting the lower

> courts to rewrite Fourth Amendment law in this area.

As I read these passages, I imagined that Collyer was trying to do more than 1) point to how many problems overruling the dragnet would cause and 2) uphold the dignity of the rubber stamp FISC and its 36+ previous decisions the phone dragnet is legal.

There is reason to believe she knows what we don't, at least not officially: that even within the scope of the phone dragnet, the dragnet is part of more comprehensive mosaic surveillance, because it correlates across platforms and identities. And all that's before you consider how, once dumped into the corporate store and exposed to NSA's "full range of analytic tradecraft," innocent Americans might be fingerprinted to include our lifestyles.

That is, not only doesn't Collyer see a way (because of legal boundary concerns about the dragnet generally, and possibly because of institutional concerns about FISC) to rule the dragnet illegal, but I suspect she sees the reverberations that such a ruling would have on the NSA's larger project, which very much is about building mosaics of intelligence.

No wonder the government is keeping that August 20, 2008 opinion secret, if it indeed discusses the correlations function in the dragnet, because it may well affect whether the dragnet gets assessed as part of the mosaic NSA uses it as.

Verizon's flaccid but public legal complaint

Now, you might think such language in Collyer's opinion would invite Verizon to appeal this decision. But given this lukewarm effort, it seems unlikely to do so. Consider the following details:

Leon issued his decision December 16. Verizon did not ask the FISC for guidance (which makes sense because they are only permitted to

challenge orders).

Verizon got a new Secondary Order after the January 3 reauthorization. It did not immediately challenge the order.

It only got around to doing so on January 22 (interestingly, a few days after ODNI exposed Verizon's role in the phone dragnet a second time), and didn't do several things — like asking for a hearing or challenging the legality of the dragnet under 50 USC 1861 as applied — that might reflect real concern about anything but the public appearance of legality. (Note, that timing is of particular interest, given that the very next day, on January 23, PCLOB would issue its report finding the dragnet did not adhere to Section 215 generally.)

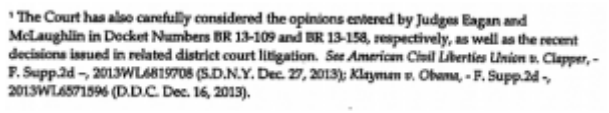
Indeed, this challenge might not have generated a separate opinion if the government weren't so boneheaded about secrecy.

Verizon's petition is less a challenge of the program than an inquiry whether the FISC has considered Leon's opinion.

> It may well be the case that this Court, in issuing the January 3,2014 production order, has already considered and rejected the analysis contained in the Memorandum Order. [redacted] has not been provided with the Court's underlying legal analysis, however, nor [redacted] been allowed access to such analysis previously, and the order [redacted] does not refer to any consideration given to Judge Leon's Memorandum Opinion. In light of Judge Leon's Opinion, it is appropriate [redacted] inquire directly of the Court into the legal basis for the January 3, 2014 production order,

As it turns out, Judge Thomas Hogan (who will take over the thankless presiding judge position from Reggie Walton next month) did consider Leon's opinion in his January 3 order, as he

noted in a footnote.



[1] The Court has also carefully considered the opinions entered by Judges Eagan and McLaughlin in Docket Numbers BR 13-109 and BR 13-158, respectively, as well as the recent decisions issued in related district court litigation. *See American Civil Liberties Union v. Clapper*, - F. Supp.2d –, 2013WL6819708 (S.D.N.Y. Dec. 27, 2013); *Klayman v. Obama*, - F. Supp.2d -, 2013WL6571596 (D.D.C. Dec. 16, 2013).

And that's about all the government said in its response to the petition (see paragraph 3): that Hogan considered it so the FISC should just affirm it.

Verizon didn't know that Hogan had considered the opinion, of course, because it never gets Primary Orders (as it makes clear in its petition) and so is not permitted to know the legal logic behind the dragnet unless it asks nicely, which is all this amounted to at first.

Note that the government issued its response (as set by Collyer's scheduling order) on February 12, the same day it released Hogan's order and its own successful motion to amend it. So ultimately this headache arose, in part, because of the secrecy with which it treats even its most important corporate spying partners, which only learn about these legal arguments on the same schedule as the rest of us peons.

Yet in spite of the government's effort to dismiss the issue by referencing Hogan's footnote, Collyer said because Verizon submitted a petition, "the undersigned Judge must consider the issue anew." Whether or not she was really required to or could have just pointed to the footnote that had been made public, I don't know. But that is how we got this new opinion.

Finally, note that Collyer made the decision to unseal this opinion on her own. Just as interesting, while neither side objected to doing so, Verizon specifically suggested the opinion could be released with no redactions, meaning its name would appear unredacted.

> The government contends that certain information in these Court records (most notably, Petitioner's identity as the recipient of the challenged production order) is classified and should remain

> redacted in versions of the documents that are released to the public. See Gov't Mem. at 1. Petitioner, on the other hand, "request[s] no redactions should the Court decide to unseal and publish the specified documents." Pet. Mem. at 5. Petitioner states that its petition "is based entirely on an assessment of [its] own equities" and not on "the potential national security effects of publication," which it "is in no position to evaluate." Id.

I'll return to this. But understand that Verizon wanted this opinion — as well as its own request for it — public.

I'll return to the apparent fact that Verizon is trying to get credit for challenging the dragnet, after 8 years of not doing so. But consider one other notable detail of this case.

I can see why Verizon made the effort to inquire about Leon's ruling, given that Larry Klayman got standing because he's a Verizon subscriber. But note, Klayman only claims to be **a Verizon cell subscriber**, not a Verizon landline subscriber (as ACLU is). Someone has been running around leading top journalists to believe that the NSA doesn't get cell data, or at least not cell data from non-AT&T providers, and that since Verizon Wireless is gaining more and more of the market share, that means NSA is getting less and less coverage of cell traffic.

But if Verizon is not providing cell data to the NSA (via some means, whether Section 215 or another), then it shouldn't care about the Leon ruling because it doesn't actually change its legal exposure, since the ruling only pertains to cell data which according to reports is purportedly not collected under Section 215. That doesn't mean it wouldn't want to make a public show of caring about the dragnet anyway, given its ongoing exposure and uncertainties about the boundaries of the dragnet. But the detail is worth noting.

The collective Fourth Amendment

In other words, by all appearances (heh) this effort was a publicity stunt on Verizon's part, not a real concern about the legality of their participation in the dragnet (though I do look forward to a similar publicity stunt raising PCLOB's concerns about the statutory compliance).

Which is a pity because of another argument that only Verizon (or another of the telecoms even less likely to raise it) might be able to challenge on appeal.

Collyer dismissed any concern about the bulk of the orders involved using the same argument Judge Jeffrey Miller used to rebut Basaaly Moalin's concerns about the scope of the dragnet: because Fourth Amendment Rights are individual, only an individual enjoys Fourth Amendment protection, not the aggregate group affected by a dragnet.

> Judge Leon also repeatedly emphasized the total quantity of telephony metadata obtained and retained by NSA. That focus is likewise misplaced under settled Supreme Court precedent. The Court has repeatedly reaffirmed that Fourth Amendment rights are "personal rights" that "may not be vicariously asserted." See Rakas v. Illinois, 439 U.S. 128, 133-134 (1978) (citing cases; citations and internal quotation marks omitted); accord Minnesota v. Carter, 525 U.S. 83, 88 (1998). Accordingly, the aggregate scope of the collection and the overall size of NSA's database are immaterial in assessing whether any person's reasonable expectation of privacy has been violated such that a search under the Fourth Amendment has occurred. To the extent that the quantity of metadata is relevant, it is relevant only on a user-by-user basis. The pertinent question is whether a particular user has a reasonable

> expectation of privacy in the telephony metadata associated with his or her own calls.

But that logic seems to utterly ignore who the petitioner here is: not you and me and ACLU and Larry Klayman, but Verizon, who provides all of us one or another kind of phone service, and has therefore been granted the specific legal right to vicariously assert our Fourth Amendment rights for us.

Collyer analyzes and grants Verizon standing in two different ways here. As a second step, she points to both the language in 50 USC 1861 and the precedent in In Re Directives (which found that Yahoo had standing to challenge multiple Directives under Protect America Act) to rule that Congress envisioned Verizon having standing to challenge any range of illegality.

> The Court is also satisfied that Congress has [redacted] as the recipient of a Section 1861 production order, the right to bring a challenge in this Court **to enforce the rights of its customers**. As noted above, FISA states that the recipient of a Section 1861 production order "may challenge the legality of that order by filing a petition" with the FISC. 50 U.S.C. § 1861(f)(2)(A)(i). As with the similar provision in In Re Directives, Section 1861(f) "does nothing to circumscribe the types of claims of illegality that can be brought." In Re Directives, 551 F.3rd at 1009 (discussing now-expired 50 U.S.C. § 1805b(h)(1)A)), the PAA provision described above in not 6). Indeed, it provides that this Court may modify or set aside a production order "if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful," thus suggesting that Congress intended to permit the recipients of production orders to bring a range of challenges.

> [my emphasis]

So the petitioner here is not you and me and ACLU and Klayman separately, but Verizon, representing at least its 40 million landline subscribers and possibly (if they're included in the dragnet) its 103 million cell phone subscribers. I'm not a lawyer, but it seems that even at this level, Verizon's complaint necessarily encompasses tens of millions and probably hundreds of millions of people that, because Verizon is the only entity guaranteed to have standing, must be represented in aggregate.

Moreover, Collyer **on her own** asserts (citing back to In Re Directives) that Verizon has been harmed here.

> To have standing under Article III of the Constitution, "the suitor must plausible allege that it has suffered an injury, which was caused by the defendant, and the effects of which can be addressed by the suit." [reference to Directives citing Warth] The Court is satisfied [redacted] has Article III standing here. Like [redacted] "faces an injury in the nature of the burden it must shoulder" to provide the Government with call detail records. Id. That injury is "obviously and indisputably caused by the [G]overnment" through the challenged Secondary Order, and this Court is capable of redressing the injury by vacating or modifying the order.

Thus, it's not just that Verizon necessarily represents all of our collective Fourth Amendment rights as the entity Congress has given clear standing to, but according to Collyer it has suffered injury in its provision of all our call records.

Verizon didn't argue any of this. Collyer did, on her own (that's what you can do in secret

courts, I guess). I'm sure Verizon will find it very useful if the government starts requiring Verizon to keep business records it currently doesn't, which is probably the problem with the dragnet and cell phone problem anyway. But for now, in its flaccid publicity stunt, Verizon seems to have shown no interest in the unique Fourth Amendment considerations raised by asserting the rights of up to 143 million customers, almost half the United States.

But at the core of Collyer's argument is both the affirmation that Verizon can vicariously assert our Fourth Amendment rights — it is the only one who explicitly can, according to Congress — and that precedents that apply to individual cars and homes at the same time prohibit Verizon from vicariously asserting our Fourth Amendment rights.

That doesn't make any sense! Collyer has laid out both its own individual injury as Verizon serving us all, as well as its vicarious ability to "enforce the rights of its customers," plural.

Again, I'm not a lawyer, so have no idea whether this would fly. But if it would, it'd sure be nice to see Verizon go beyond publicity stunts and really enforce our rights, as only it can do.

Which is why it's unfortunate that Verizon seems primarily interested in publicity stunts, not aggressive legal challenges.

Update: Date for presumed correlations opinion fixed.