THE AWKWARD TIMING OF THE 2ND CIRCUIT DENIAL OF ACLU'S REQUEST FOR A PHONE DRAGNET INJUNCTION

The 2nd circuit just denied the ACLU's request for an injunction in the phone dragnet, finding that Congress intended to let the dragnet continue for 6 months after passage of USA F-ReDux.

That's not all that surprising, but it also means the 2nd circuit is dodging constitutional issues for now (in part by claiming Congress had adopted their reasoning on the meaning of "relevant to," which it did not; I will return to this).

But the court remanded the case on one main issue: what happens on November 29, when the 6 month transition period ends.

> Appellants and the government disagree, however, regarding the mootness of the final relief requested after November 29: an injunction that would require the government to end the telephone metadata program and purge records collected unlawfully. Appellants argue that the government intends to retain the records "indefinitely," and are under no outside obligation to purge them, and thus that their claims for relief will not become moot on November 29. The government argues that the claims will be moot on November 29, because the telephone metadata program will cease at that time, and an order enjoining the telephone metadata program will have no effect.
>
> Further, the government notes that the Office of the Director of National

> Intelligence has announced that the government will not use § 215 data for law enforcement or investigatory purposes after November 29. See Statement by the ODNI on Retention of Data Collected Under Section 215 of the USA PATRIOT Act (July 27, 2015). Additionally, the government states that it will destroy all records as soon as possible after the government's litigation-preservation obligations end, id., and thus Appellants' requests that their information no longer be queried and that their records be purged will also be moot.
>
> [snip]
>
> We do not address whether Appellants' claims will become moot on November 29, and leave this, and all other remaining questions, to the district court in the first instance.

While I don't expect much to come of this question either, it is rather awkward that the court has chosen to remand that decision *today*, of all days.

As it is, the 2nd circuit misses one development in this case, which is that after declaring on July 27 that they were going to keep the data but not use it for law enforcement purposes, the FISC then refused the government's request to just rubber stamp that decision. So the question of what will happen with the data is still being review at the FISC.

Not only that, but today is also the deadline Michael Mosman set for FISC-appointed amicus Preston Burton to submit his first brief on this question.

So Burton will submit something — there's no reason to think we'll get to see all of his brief — without the benefit of knowing that ACLU may still contest whatever he argues for

regarding the use of the data past November 29. And of course, one reason the government may need to keep that data past November 29 is because EFF has a protection order that requires they keep it for their lawsuit(s).

That still doesn't mean anything all that interesting will come of this, but we do have two courts addressing the same question at the same time, without full notice of the other.

I CON THE RECORD: DROP THE LAWSUITS AND WE'LL RELEASE THE DATA HOSTAGES

I Con the Record just announced that the NSA will make the phone dragnet data it has "analytically unavailable" after the new system goes live in November, and unavailable even to techs three months later.

> On June 29, 2015, the Foreign Intelligence Surveillance Court approved the Government's application to resume the Section 215 bulk telephony metadata program pursuant to the USA FREEDOM Act's 180-day transition provision. As part of our effort to transition to the new authority, we have evaluated whether NSA should maintain access to the historical metadata after the conclusion of that 180-day period.
>
> NSA has determined that analytic access to that historical metadata collected under Section 215 (any data collected before November 29, 2015) will cease on November 29, 2015. However, solely for data integrity purposes to verify the records produced under the new targeted

> production authorized by the USA FREEDOM Act, NSA will allow technical personnel to continue to have access to the historical metadata for an additional three months.
>
> Separately, NSA remains under a continuing legal obligation to preserve its bulk 215 telephony metadata collection until civil litigation regarding the program is resolved, or the relevant courts relieve NSA of such obligations. The telephony metadata preserved solely because of preservation obligations in pending civil litigation will not be used or accessed for any other purpose, and, as soon as possible, NSA will destroy the Section 215 bulk telephony metadata upon expiration of its litigation preservation obligations.

As I understand it, whatever data has been found to be two or three degrees of separation from a baddie will remain in NSA's maw, but the data that has never returned off a search will not.

I'm pleasantly surprised by this, as I suspect it reflects a decision to accept the Second Circuit verdict in ACLU v. Clapper and to move to shut down other lawsuits.

As I noted, two weeks ago, the ACLU moved for an injunction against the dragnet, which not only might have led to the Second Circuit ordering the government to purge ACLU's data right away (and possibly, to stop collecting all data), but also basically teed up the Second Circuit to remind the FISC it is not an appellate court. I worried that would lead the FISC to ask FISCR to review its dragnet decisions under a provision newly provided under the USA F-ReDux.

Shortly after ACLU filed its request for an injunction, the government asked for an extension to … today, which the court granted.

So I assume we'll shortly see that filing arguing that, since the government has

voluntarily set a purge date for all the dragnet data, ACLU should not get its injunction.

That doesn't necessarily rule out a FISCR fast track request, but I think it makes it less likely.

The other player here, however, is the EFF.

I believe both ACLU and EFF's phone dragnet client Council on American Islamic Relations, had not only standing as clients of dragnetted companies, but probably got swept up in the two-degree dragnet. But CAIR probably has an even stronger case, because it is public that FISC approved a traditional FISA order against CAIR founder Nihad Awad. Any traditional FISA target has *always* been approved as a RAS seed to check the dragnet, and NSA almost certainly used that more back when Awad was tapped, which continued until 2008. In other words, CAIR has very good reason to suspect the entire organization has been swept up in the dragnet and subjected to all of NSA's other analytical toys.

EFF, remember, is the one NGO that has a preservation order, which got extended from its earlier NSA lawsuits (like Jewel) to the current dragnet suit. So when I Con the Record says it can't destroy all the data yet, it's talking EFF, and by extension, CAIR. So this announcement — in addition to preparing whatever they'll file to get the Second Circuit off its back — is likely an effort to moot that lawsuit, which in my opinion poses by far the biggest threat of real fireworks about the dragnet (not least because it would easily be shown to violate a prior SCOTUS decision prohibiting the mapping of organizations).

We'll see soon enough. For the moment, though, I'm a bit surprised by the cautious approach this seems to represent.

Update: Timeline on data availability fixed.

Update: Here's the government's brief submitted today. I'm rather intrigued by how often the brief claims USA F-ReDux was about bulk

"telephony" data when it was supposed to be about all bulk collection. But I guess I can return to that point.

Update: They depart from describing USA F-ReDux as a ban bulk collection of telephony when they describe it as a ban on collection of bulk collection under Section 215, also not what the bill says.

> Part of the compromise on which Congress settled, which the President supported, was to add an unequivocal ban on bulk collection under Section 215 specifying that "[n]o order issued under" Section 215(b)(2) "may authorize collection of tangible things without the use of a specific selection term that meets the requirements" of that subsection.

Update: This is key language — and slightly different from what they argued before FISC. I will return to it.

> Plaintiffs assert that, by not changing the language of Section 215 authorizing the collection of business records during the transition period, Congress implicitly incorporated into the USA FREEDOM Act this Court's opinion holding that Section 215 did not authorize bulk collection. See Pls.' Mot. 7- 8. Plaintiffs rely on language providing that the legislation does not "alter or eliminate the authority of the Government to obtain an order under" Section 215 "as in effect prior to the effective date" of the statute. USA FREEDOM Act § 109, 129 Stat. at 276. That language does not advance plaintiffs' argument, however, because the statute says nothing expressly about what preexisting authority the government had under Section 215 to obtain telephony metadata in bulk. It is implausible that Congress employed the word "authority" to signify that the

> government lacked authority to conduct the Section 215 bulk telephony-metadata program during the 180-day transition period, contrary to the FISC's repeated orders and the Executive Branch's longstanding and continuing interpretation and application of the law, and notwithstanding the active litigation of that question in this Court. That is especially so because language in the USA FREEDOM Act providing for the 180-day transition period has long been a proposed feature of the legislation. It is thus much more plausible that the "authority" Congress was referring to was not the understanding of Section 215 reflected in this Court's recent interpretation of Section 215, but rather the consistent interpretation of Section 215 by 19 different FISC judges: to permit bulk collection of telephony metadata.

THE TIMING OF THE CONTEMPLATED UPSTREAM CYBER-GRAB

There's an aspect missing thus far from the discussion of NSA's possible bid for a cyber certification under Section 702 for primary use in the collection of attack signatures that could not be attributed to a foreign government.

The timing.

The discussion of creating a new Section 702 certificate came in the aftermath of the 6-month back and forth between DOJ and the FISA Court over NSA having collected US person data as part of its upstream collection (for more

detail than appears in the timeline below, see this post). During that process, John Bates ruled parts of the program – what he deemed the *intentional* collection of US person data within the US – to be unconstitutional. That part of his opinion is worth citing at length, because of the way Bates argues that the inability to detach entirely domestic communications that are part of a transaction does not mean that those domestic communications were "incidentally" collected. Rather, they were "intentionally" collected.

> Specifically, the government argues that NSA is not "intentionally" acquiring wholly domestic communications because the government does not intend to acquire transactions containing communications that are wholly domestic and has implemented technical means to prevent the acquisition of such transactions. See June 28 Submission at 12. This argument fails for several reasons.
>
> NSA targets a person under Section 702 certifications by acquiring communications to, from, or about a selector used by that person. Therefore, to the extent NSA's upstream collection devices acquire an Internet transaction containing a single, discrete communication that is to, from, or about a tasked selector, it can hardly be said that NSA's acquisition is "unintentional." In fact, the government has argued, that the Court has accepted, that the government intentionally acquires communications to and from a target, even when NSA reasonably – albeit mistakenly – believes that the target is located outside the United States. See Docket No. [redacted]
>
> [snip]
>
> The fact that NSA's technical measures cannot prevent NSA from acquiring

> transactions containing wholly domestic communications under certain circumstances does not render NSA's acquisition of those transactions "unintentional."
>
> [snip]
>
> [T]here is nothing in the record to suggest that NSA's technical means are malfunctioning or otherwise failing to operate as designed. Indeed, the government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server.
>
> [snip]
>
> By expanding its Section 702 acquisitions to include the acquisition of Internet transactions through its upstream collection, NSA has, as a practical matter, circumvented the spirit of Section 1881a(b)(4) and (d)(1) with regard to that collection. (44-45, 48)

There are a number of ways to imagine that victim-related data and communications obtained with an attack signature might be considered "intentional" rather than "incidental," especially given the Snowden document acknowledging that so much victim data gets collected it should be segregated from regular collection. Add to that the far greater likelihood that the NSA will unknowingly target domestic hackers — because so much of hacking involves obscuring attribution — and the likelihood upstream collection targeting hackers would "intentionally" collect domestic data is quite high.

Plus, there's nothing in the 2011 documents released indicating the FISC knew upstream

collection included cyber signatures — and related victim data — in spite of the fact that "current Certifications already allow for the tasking of these cyber signatures." No unredacted section discussed the collection of US person data tied to the pursuit of cyberattackers that appears to have been ongoing by that point.

Similarly, the white paper officially informing Congress about 702 didn't mention cyber signatures either. There's nothing public to suggest it did so after the Senate rejected a Cybersecurity bill in August, 2012, either. That bill would have authorized less involvement of NSA in cybersecurity than appears to have already been going on.

With all that in mind, consider the discussions reflected in the documents released last week. The entire discussion to use FBI's stated needs to apply as backup to apply for a cyber certificate came at the same time as NSA is trying to decide what to do with the data it illegally collected. Before getting that certificate, DOJ approved the collection of cyber signatures under other certificates. It seems likely that this collection would violate the spirit of the ruling from just the prior year.

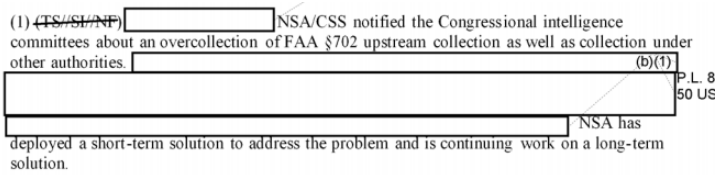
And NSA's assistance to FBI may have violated the prior year's orders in another way. SSO contemplated delivering all this data directly to FBI.

> (S//REL) All data (metadata and/or content) collected under the auspices of these FISC orders will be forwarded securely and directly to the designated FBI repository. The FISC orders do contain a provision, as follows: "NCIJTF personnel participating in this joint investigation may have access to raw data prior to minimization." However, access to raw data by NTOC members of the NCIJTF will be facilitated under the purview of the FBI and not through any actions that SSO might take as the collected data passes through NSA's secure Wide Area Networks. Should the FBI's cyber orders from the FISC be modified in the future to authorize raw data retention by NSA, SSO will coordinate with all cognizant NSA offices (e.g., Data Governance, OGC, SV) to ensure the proper data delivery mechanism is put in place.

Yet one of the restrictions imposed on upstream collection — voluntarily offered up by DOJ — was that no raw data from NSA's upstream collection go to FBI (or CIA). If there was uncertainty where FBI's targeting ended and NSA's began, this would create a violation of prior orders.

Meanwhile, the reauthorization process had already started, and as part of that (though curiously timed to coincide with the release of DOJ's white paper on 702 collection) Ron Wyden and Mark Udall were trying to force NSA to figure out how much US person data they were collecting. Not only did the various Inspectors General refuse to count that data (which would have, under the logic of Bates' opinions finding that illegally collected data was only illegal if the government knew it was US person data, made the data illegal), but the Senate Intelligence Committee refused to consider reconstituting their Technical Advisory Committee which might be better able to assess whether NSA claims were correct.

Sometime in that period, just as Wyden was trying to call attention to the fact that NSA was collecting US person data via its upstream collection, NSA alerted the Intelligence Committees to further "overcollection" under upstream collection.


(1) ~~(TS//SI//NF)~~ [redacted] NSA/CSS notified the Congressional intelligence committees about an overcollection of FAA §702 upstream collection as well as collection under other authorities. [redacted] (b)(1) [redacted] P.L. 8 50 US [redacted] NSA has deployed a short-term solution to address the problem and is continuing work on a long-term solution.

As I suggested here, the length of the redaction and mention of "other authorities" may reflect the involvement of another agency like FBI. One possibility, given the description of FBI collecting on cyber signatures using both PRTT and (presumably) traditional FISA in the discussions of SSO helping the FBI conduct this surveillance (note, I find it interesting though not conclusive that there is no mention of Section 215 to collect cybersecurity data), is that the initial efforts to go after these signatures in some way resulted in overcollection. If FISC interpreted victim-related data to be overcollection — as would be unsurprising under Bates' 2011 upstream opinion — then it would explain the notice to Congress.

One more point. In this post, I noted that USA

F-ReDux authorized FISC to let the government use data it had illegally collected but which FISC had authorized by imposing additional minimization procedures. It's just a wildarseguess, but I find it plausible that this 2012 overcollection involved cyber signatures (because we know NSA was collecting it and there is reason to believe it violated Bates' 2011 opinion), and that any victim data now gets treated under minimization procedures and therefore that any illegal data from 2012 may now, as of last week, be used.

All of which is to say that the revelation of NSA and FBI's use of upstream collection to target hackers involves far more legal issues than commentary on the issue has made out. And these legal issues may well have been more appropriate for the government to reveal before passage of USA F-ReDux.

Update, 11/6: Some dates added from this opinion.

May 2, 2011: DOJ Clarification to FISC letter first admits MCT problem.

May 5, 2011: Government asks for extension until July 22, 2011.

Mid-2011: NSA's Special Source Operations becomes aware of FBI's intent to seek orders involving telecom infrastructure.

July 8, 2011: Court (John Bates) meets with senior DOJ people, tells them he has serious concerns.

July 14, 2011: Government files another extension; court grants extension to September 20, 2011.

September 13, 2011: In filing submitted in response to Bates request, government refuses to count entirely US person content collected under upstream collection.

September 14, 2011: Court extends deadline to

October 10, 2011.

October 3, 2011: John Bates rules parts of upstream 702 unconstitutional.

Before October 6, 2011:
Government considers appealing Bates ruling.

October 13, 2011: Bates issues briefing order on illegally collected upstream data. Government responds by arguing 1809(a)(2) doesn't apply to it.

October 31, 2011: Bates approves new minimization procedures accounting for MCT problem but apparently not cyber collection.

December 9, 2011: PRTT order expires without renewal, NSA discontinues PRTT Internet dragnet and destroys all data.

December 20, 2011: FBI requests access to NSA's "access to infrastructure established by NSA for collection of foreign intelligence from U.S. telecommunications providers" to carry out FISA cyber orders (both Pen Register and content) targeting IP addresses.

December 21, 2011: SSO prepares approval form for assistance to FBI.

Late 2011: Government decides to start mitigating upstream 702 data.

January 2012: Obama reconfirms Transit Program.

March 23, 2012: New Cyber Certificate in the works.

March 27, 2012: SID Director Theresa Shea signs off on staff processing form for assistance to FBI.

April 2012: Government orally informs Bates it will purge upstream 702 data collected prior to October 31, 2011.

May 2012: DOJ approves targeting certain signatures under FAA FG Certificate.

May 4, 2012: DOJ informs Congress about 702 (including notice of MCT problem) in

anticipation of 702 reauthorization. DOJ does *not* tell Congress NSA is using upstream 702 to collect on anything but email and phone identifiers.

May 4, 2012: Ron Wyden and Mark Udall request Charles McCullough to investigate how many Americans have been caught in upstream collection.

May 22, 2012: SSCI marks up FAA Reauthorization, rules Wyden amendment to reconstitute SSCI Technical Advisory Group to examine FAA out of order.

June 6, 2012: George Ellard tells Wyden a request for number of Americans caught in upstream collection is not possible and would violate the privacy of Americans.

June 16, 2012: Wyden releases McCullough's public response.

July 2012: DOJ approves targeting certain IP addresses under FAA.

July 1 to September 30, 2012: NSA informs Congress about upstream Section 702 (and other authority) overcollection.

August 2, 2012: Cybersecurity Bill of 2012 fails cloture vote.

August 24, 2012: Government submits first document for reauthorization and amendment (without mention of new certificate): "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications."

September 20, 2012: FISC first approves minimization procedures allowing FBI to share of information it believes may mitigate or prevent cyber intrusions with private entities. Note, it's possible this change also applied to NSA, but that does not appear in the unredacted discussion. If it only applies to FBI, it should

pertain to PRISM production, as FBI doesn't (or didn't) get unminimized upstream data.

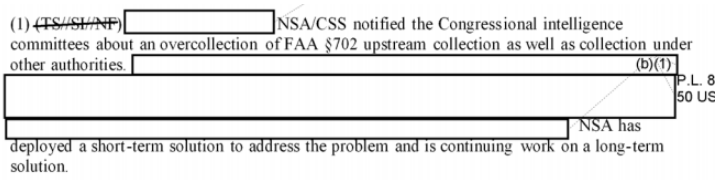
December 2012: FAA extended until December 31, 2017.

August 30, 2013: FISC approves revised language permitting FBI (unclear whether this also includes NSA) sharing of cyber threat information with private entities.

NSA REPORTED A SECTION 702 UPSTREAM OVERCOLLECTION INCIDENT IN 2012

I'm working on a longer post on the timing of the NSA's bid to get a cyber Section 702 certificate in 2012. But I wanted to point to a detail about upstream 702 collection that may be relevant to the issue.

According to the 4Q FY2012 Intelligence Oversight Board report — the one covering the quarter ending September 30, 2012 — NSA notified Congress of an overcollection (a polite way of saying "illegal data collection") under both upstream collection and "other authorities." The overcollection was fairly significant, both because NSA *did* notify Congress, which it doesn't do for individual incidences of overcollection, and because NSA had to implement both a short-term and long-term solution to the collection issue.


(1) ~~(TS//SI//NF)~~ [redacted] NSA/CSS notified the Congressional intelligence committees about an overcollection of FAA §702 upstream collection as well as collection under other authorities. [redacted] (b)(1) P.L. 8 50 US [redacted] NSA has deployed a short-term solution to address the problem and is continuing work on a long-term solution.

This is almost certainly separate from the

upstream violations reported in 2011, which resulted in Judge John Bates declaring the collection of entirely US-person data as part of Multi-Communication Transactions collected using upstream 702 collection to be a violation of the Fourth Amendment. Reference to that notice appeared in the 3Q FY2011 report, the one covering the quarter ending June 30, 2011. Not only does the earlier IOB Report show Congress had already been notified of the 2011 violations, but that (unlike some earlier notices) they were notified in timely fashion.

Which suggests the 2012 notification was probably provided to Congress shortly after its official discovery, too.

Moreover, a description of the 2011 problems with upstream collection appeared in a May 4, 2012 letter to Congress, in anticipation of FISA Amendments Act reauthorization that year, by which point NSA had already informed Bates they were going to purge the overcollected MCT data (that happened in April 2012). Thus, no *new* notice would have been necessary (and would have been sent exclusively to the Intelligence Committees) in 3Q FY2012, which started on July 1.

So this 2012 notice almost certainly represents yet another incidence where NSA (and possibly another agency, given the redaction length and reference to other authorities) illegally collected content it wasn't entitled to collect inside the US.

This overcollection is significant for two reasons.

First, as will become more clear when I do this timeline, DOJ and NSA would have been dealing with this overcollection at precisely the same time the two agencies were preparing to apply for a Section 702 certification authorizing the collection of cyber signatures. Indeed, it's possible that is why this overcollection was officially identified, as I'll lay out, though there are plenty of other possibilities as well.

Just as importantly, USA F-ReDux probably just authorized the government to use the data collected under this second incident of apparently systemic overcollection under upstream 702.

On its face, Section 301 of USA F-ReDux *appears* to prohibit the use (but not the parallel construction of) data collected unlawfully under Section 702 unless it presents a threat of death or serious bodily harm (which NSA has secretly redefined to include threat to property).

> [I]f the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial [… or any other Federal proceeding …] except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

But in substance, the Section actually authorizes the government to use such data once it has satisfied the FISC.

> If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.

The Section likely addresses something that happened as John Bates tried to deal with both the PRTT Internet dragnet violations in 2010 and the upstream collection violations in 2011. In

both cases, he found the government had intentionally collected US person content in the US. And so, Bates determined, under 50 U.S.C. § 1809(a), it would be a crime for the government to disseminate the data.

In 2010, Bates rejected a slew of government arguments (see pages 100 to 113) that he could just retroactively make this illegal collection legal.

> Finally, insofar as the government suggests that the Court has an inherent authority to permit the use and disclosure of all unauthorized collection without regard to Section 1809, see Memorandum of Law at 73-74 & n.37, the Court again must disagree.
>
> [snip]
>
> The Court simply lacks the power, inherent or otherwise, to authorize the government to engage in conduct that Congress has unambiguously prohibited

Bates' interpretation of 50 U.S.C. § 1809(a) is what led the government to purge the illegally collected upstream data in April 2012 (that may have also been why NSA purged its illegally collected Internet dragnet data in December 2011).

Section 301 of USA F-ReDux was clearly intended to give FISC the authority Bates said he didn't have in 2010: to permit a FISC judge to permit the government to disseminate data found to be illegally collected, but retroactively sanctioned via the use of minimization procedures.

At first, I didn't think the Section would affect any known data, because NSA purged both the illegal PRTT data and the illegal upstream data, so that couldn't be used anymore.

But the IOB report shows there was *more* illegal upstream data collected, within a year. And the reference to a "long-term solution" to it may

suggest that NSA held onto the data and was just finding a way to retroactively authorize it.

From the IOB description, we can't know *what* data NSA had illegally collected or why. But there's a decent chance USA F-ReDux just retroactively made the use of it legal.

SONY, THE WHITE HOUSE, AND 10 DOWNING STREET: WHAT'S THE QUID PRO QUO?

Lots of ugly things crawled out of Sony Pictures Entertainment's emails leaked by hackers this past autumn.

The leak of emails and intellectual property, including then-unreleased film The Interview, was labeled "a serious national security matter" by the White House. In January this year, President Obama issued an executive order increasing sanctions against North Korea, the purported origin of the hack on SPE's network and computers.

Sony Pictures Entertainment (SPE) is a wholly-owned subsidiary of Sony Corporation, a Japanese multinational conglomerate. In offering retaliation on behalf of SPE, the White House

placed SPE on par with critical U.S. infrastructure, though no one will be physically injured or die should SPE be hacked again, and the market won't collapse if SPE loses money on all its movies this year.

If SPE, a foreign-owned, information security-challenged entertainment firm, is now entitled to military protection against cyberattack, what is it the White House and the U.S. will receive or has received in exchange?

What's the exchange in this quid pro quo?

Which brings us to the matter of STARZ' cable series, Outlander, and UK Prime Minister David Cameron's government.

In 2013, STARZ network ordered the 16-episode adaptation of bestselling historical fiction novel, Outlander by author Diana Gabaldon, from production companies Tall Ship Productions, Story Mining & Supply Co., and Left Bank Productions, in association with Sony Pictures Television.

While STARZ was the U.S. distributor, offering the series on its own cable network, SPE's TV arm appears to have handled overseas distribution to broadcast, cable, and video streaming services.

Outlander's cross-genre narrative is set mainly in 1740s Scotland; the story is sympathetic to a Scottish protagonist and his time-traveling English wife who are caught between the British and Jacobites in the ramp up to the 1746 Battle at Culloden. The Scottish people and countryside are treated favorably in the series' production.

The program debuted on STARZ in the U.S. on August 9 last year – a little less than six weeks before Scotland's independence referendum ("IndyRef"). Outlander began airing in Canada and Australia in August also, and in October in Ireland after the IndyRef vote.

Distribution deals in other countries including Germany, Hungary, Japan, and the Netherlands led

to wider release overseas last year.

But Outlander never received a distribution deal in 2014 in the UK, in spite of its many Scottish and British fans' clamor and the source book's status as a renewed bestseller in advance of the show's U.S. debut. To date the series has only released on Amazon Prime Instant Video in the UK, for paid video-on-demand streaming – not on broadcast or cable.

At least one email leaked by hackers revealed that SPE personnel had a meeting or meetings with Cameron's government. In an internal email from Keith E. Weaver, executive vice president, SPE executives were told,

> "Your meeting with Prime Minister Cameron on Monday will likely focus on our overall investment in the U.K. – with special emphasis on the jobs created by Tommy Cooper [the ITV show], the importance of Outlander (i.e., particularly vis-a-vis the political issues in the U.K. as Scotland contemplates detachment this Fall), and the growth of our channels business…"

The implication is that SPE would suppress any effort to distribute Outlander to the benefit of Cameron's anti-independence position, in exchange for "growth of our channels business…"

What exactly does this mean?

And is the pursuit of growth confined to SPE, or did "channels business" mean something else? Were Sony executives also looking for opportunities for Sony Corporation, which includes Sony Computer Entertainment, Sony Music Entertainment, Sony Mobile Communications (once known as Sony Ericsson), and Sony Financial?

Did SPE executives and the Prime Minister agree not to seek broadcast or cable distribution Outlander in the UK before this month's election?

It's bad enough that SPE may have mislead

Outlander's other production companies as well as author Gabaldon, who believed that a UK distribution deal was being sought as of last summer.

But this sustained suppression of content based on historic fact, to reduce friction against Cameron's government, is beyond the pale.

Think about it: Was Cameron so worried about the outcome of not only Scotland's independence referendum, but his Conservative Party's performance in this week's upcoming UK election, such that he negotiated a deal with a U.S.-supported Japanese-owned entertainment company to suppress a cable television series featuring a positive Scottish sentiment?

Recall what SPE president Michael Lynton said about the theatrical release of The Interview this past Christmas:

> ''We have never given up on releasing 'The Interview,''' Lynton said in a statement Tuesday. ''While we hope this is only the first step of the film's release, we are proud to make it available to the public and to have stood up to those who attempted to suppress free speech.''

Apparently SPE's okay with trampling creators' free speech provided there's a quid pro quo negotiated in the Queen's English with a foreign government.

The undisclosed quid pro quos may explain, though, why Sony Corporation hasn't booted SPE president Lynton out on his ass. One would think that a business whose core product is digitized intellectual property would have placed more resources and effort on information security, rather than spending $20 million a year on membership fees to the Motion Picture Association of America for lobbyists protecting their intellectual property rights. And one would think that a major failure like the 2014 email hack would have resulted in an executive

purge at SPE.

Having kept Lynton on board, what exactly did parent Sony Corporation get out of the hack, or out of negotiations with UK's PM David Cameron?

But go one step further: Do the other major film studios and their parent corporations also enter quid pro quos with governments to suppress intellectual property in exchange for undisclosed benefits?

And will Sony and its subsidiaries, along with the other major film studios and their parents, seek more quid pro quo arrangements from within U.S. government-established and protected Information Sharing and Analysis Organizations, as outlined by President Obama's Executive Order 13691, signed after increasing sanctions against North Korea?

A GUIDE TO THE 5+ KNOWN INTELLIGENCE COMMUNITY TELECOMMUNICATIONS METADATA DRAGNETS

I've been laying this explanation out since USA Today provided new details on DEA's International Dragnet, but it's clear it needs to be done in more systematic fashion, because really smart people continue to mistakenly treat the Section 215 database as the analogue to the DEA dragnet described by USAT, which it's not. There are at least five known telecommunications dragnets (some of which appear to integrate other kinds of metadata, especially Internet metadata). Here's a quick guide to what is known about each (click to enlarge, let me know of corrections/additions, I will do running updates

to make this more useful):

	NSA	DEA	CIA	FBI
International	**EO 12333 / SPCMA** • Includes Internet metadata • Analysts need only FI purpose, including CN • Since 2008 permitted chaining on USPs, but not targeting them • Standard minimization procedures • Chains across metadata type • Linked into automatic analysis • Probably includes location data	**USTO: 21 USC 876** (DEA's "tangible things" subpoenas) • Ostensibly counternarcotics purpose, but used for other purposes (included counterproliferation) • Linked into automatic analysis • Location data inclusion unclear • Allegedly shut down in September 2013	**PROTON** (predecessor to ICREACH) Chains across metadata type **AT&T** voluntary production of foreign calls	
Domestic	**Section 215** • Limited to counterterrorism purpose • Strict dissemination limitations • First Amendment review for chaining • Chaining permitted on USPs • Linked into automatic analysis until 2009; NSA has given up effort to return to automatic chaining • Currently limited to pre-approved or emergency queries (~300 identifiers queried multiple times)	**Hemisphere** (provider based, may be limited to AT&T backbone) • Ostensibly counternarcotics purpose, but used by other agencies • Includes analysis involving location data		**Exigent Letters** Onsite telecom presence from 2002-2006 Ongoing **TCAU** contracts with AT&T and another telecom; AT&T provides enhanced services

NSA, International

When people think about the NSA dragnet they mistakenly think exclusively of Section 215. That is probably the result of a deliberate strategy from the government, but it leads to gross misunderstanding on many levels. As Richard Clarke said in Congressional testimony last year, Section "215 produces a small percentage of the overall data that's collected."

Like DEA, NSA has a dragnet of international phone calls, including calls into the United States. This is presumably limited only by technical capability, meaning the only thing excluded from this dragnet are calls NSA either doesn't want or that it can't get overseas (and note, some domestic cell phone data may be available offshore because of roaming requirements). David Kris has said that what collection of this comes from domestic providers comes under 18 U.S.C. § 2511(2)(f). And this dragnet is not just calls: it is also a whole slew of Internet data (because of the structure of the Internet, this will include a great deal of US person data). And it surely includes a lot of other data points, almost certainly including location data. Analysts can probably access Five Eyes and other intelligence partner data, though this likely includes additional restrictions.

There are, within this dragnet, two sets of

procedures for accessing it. There is straight EO 12333, which appears to defeat US person data (so if you're contact chaining and a known US person is included in the chain, you won't see it). This collection requires only a foreign intelligence purpose (which counternarcotics is explicitly included in). Standard NSA minimization procedures apply, which — given that this is not supposed to include US person data — are very permissive.

Starting in 2008 (and probably before 2004, at least as part of Stellar Wind), specially-trained analysts are also permitted to include US persons in the contact chaining they do on EO 12333 data, under an authority call "SPCMA" for "special procedures." They can't *target* Americans, but they can analyze and share US person data (and NSA has coached analysts how to target a foreign entity to get to the underlying US data). This would be treated under NSA's minimization procedures, meaning US person data may get masked unless there's a need for it. Very importantly, this chaining is not and never was limited to counterterrorism purposes — it only requires a foreign intelligence purpose. Particularly because so much metadata on Americans is available overseas, this means NSA can do a great deal of analysis on Americans without any suspicion of criminal ties.

Both of these authorities appear to link right into other automatic functions, including things like matching identities (such that it would track "emptywheel" across all the places I use that as my uniquename) and linking directly up to content, if it has been collected.

NSA, Domestic

Then there is the Section 215 dragnet, which prior to 2006 was conducted with telecoms voluntarily producing data but got moved to Section 215 thereafter; there is a still-active Jack Goldsmith OLC opinion that says the government does not need any additional statutory authorization for the dragnet (though telecoms aside from AT&T would likely be reluctant to do so now without liability protection and compensation).

Until 2009, the distinctions between NSA's EO 12333 data and Section 215 were not maintained. Indeed, in early 2008 "for purposes of analytical efficiency," the Section 215 data got dumped in with the EO 12333 data and it appears the government didn't even track data source (which FISC made them start doing by tagging each discrete piece of data in 2009), and so couldn't apply the Section 215 rules as required. Thus, until 2009, the Section 215 data was subjected to the automatic analysis the EO 12333 still is. That was shut down in 2009, though the government kept trying to find a way to resume such automatic analysis. It never succeeded and finally gave up last year, literally on the day the Administration announced its decision to move the data to the telecoms.

The Section 215 phone dragnet can only be used for counterterrorism purposes and any data that gets disseminated outside of those cleared for BRFISA (as the authority is called inside NSA) must be certified as to that CT purpose. US person identifiers targeted in the dragnet must

first be reviewed to ensure they're not targeted exclusively for First Amendment reasons. Since last year, FISC has pre-approved all identifiers used for chaining except under emergencies. Though note: Most US persons approved for FISA content warrants are automatically approved for Section 215 chaining (I believe this is done to facilitate the analysis of the content being collected).

Two very important and almost universally overlooked points. First, analysts access (or accessed, at least until 2011) BRFISA data from the very same computer interface as they do EO 12333 data (see above, which would have dated prior to the end of 2011). Before a chaining session, they just enter what data repositories they want access to and are approved for, and their analysis will pull from all those repositories. Chaining off data from more than one repository is called a "federated" query. And the contact chaining they got — at least as recently as 2011, anyway — also included data from both EO 12333 collection and Section 215 collection, both mixed in together. Importantly, data with one-end in foreign will be redundant, collected under both EO 12333 and 215. Indeed, a training program from 2011 trained analysts to re-run BRFISA queries that could be replicated under EO 12333 so they could be shared more permissively. That said, a footnote (see footnote 13) in phone dragnet orders that has mostly remained redacted appears to impose the BRFISA handling rules on any data comingled with it, so this may limit (or have imposed new more recent limits) on contact chaining between authorities.

As I noted, NSA shut down the automatic features on BRFISA data in 2009. But once data comes back in a query, it can be subjected to NSA's "full range of analytical tradecraft," as every phone dragnet order explains. Thus, while the majority of Americans who don't come up in a query don't get subjected to more intrusive analysis, if you're 3 hops (now 2) from someone of interest, you can be — everything, indefinitely. I would

expect that to include trolling all of NSA's collected data to see if any of your other identifiable data comes up in interesting ways. That's a ton of innocent people who get sucked into NSA's maw and will continue to even after/if the phone dragnet moves to the providers.

DEA, International

As I said, the analogue to the program described by the USA Today, dubbed USTO, is *not* the Section 215 database, but instead the EO 12333 database (indeed, USAT describes that DEA included entirely foreign metadata in their database as well). The data in this program provided by domestic providers came under 21 USC 876 — basically the drug war equivalent of the Section 215 "tangible things" provision. An DEA declaration in the Shantia Hassanshahi case claims it only provides base metadata, but it doesn't specify whether that includes or excludes location. As USAT describes (and would have to be the case for Hassanshahi to be busted for sanctions violations using it, not to mention FBI's success at stalling of DOJ IG's investigation into it), this database came to be used for other than counternarcotics purposes (note, this should have implications for EO 12333, which I'll get back to). And, as USAT also described, like the NSA dragnet, the USTO also linked right into automatic analysis (and, I'm willing to bet good money, tracked multiple types of metadata). As USAT describes, DEA did far more queries of this database than of the Section 215 dragnet, but that's not analogous; the proper comparison would be with NSA's 12333 dragnet, and I would bet the numbers are at least comparable (if you can even count these automated chaining processes anymore). DEA says this database got shut down in 2013 and claims the data was purged. DEA also likely would like to sell you the Brooklyn Bridge real cheap.

DEA, Domestic

There's also a domestic drug-specific dragnet, Hemisphere, that was first exposed by a NYT article. This is not actually a DEA database at all. Rather, it is a program under the drug czar that makes enhanced telecom data available for drug purposes, while the records appear to stay with the telecom.

This seems to have been evolving since 2007 (which may mark when telecoms stopped turning over domestic call records for a range of purposes). At one point, it pulled off multiple providers' networks, but more recently it has pulled only off AT&T's networks (which I suspect is increasingly what has happened with the Section 215 phone dragnet).

But the very important feature of Hemisphere — particularly as compared to its analogue, the Section 215 dragnet — is that the telecoms perform the same kind of analysis they would do for their own purposes. This includes using location data and matching burner phones (though this is surely one of the automated functions included in NSA's EO 12333 dragnet and DEA's USTO). Thus, by keeping the data at the telecoms, the government appears to be able to do more sophisticated kinds of analysis on domestic data, even if it does so by accessing fewer records.

That is surely the instructive motivation behind Obama's decision to "let" NSA move data back to the telecoms. It'd like to achieve what it can under Hemisphere, but with data from all telecom providers rather than just AT&T.

CIA

At least as the NSA documents concerning ICREACH tell it, CIA and DEA jointly developed a sharing platform called PROTON that surely overlaps with USTO in significant ways. But PROTON appeared to reside with CIA (and FBI and NSA were late additions to the PROTON sharing). PROTON included CIA specific metadata (that is, not

telecommunications metadata but rather metadata tracking their own HUMINT). But in 2006 (these things all started to change around that time), NSA made a bid to become the premiere partner here with ICREACH, supporting more types of metadata and sharing it with international partners.

So we don't know what CIA's own dragnet looks like, just that it has one, one not bound to just telecommunications.

In addition, CIA has a foreign intelligence equivalent of Hemisphere, where it pays AT&T to "voluntarily" hand over data that is at least one-end foreign (and masks the US side unless the record gets referred to FBI).

Finally, CIA can "upload or transfer some or all" of the metadata that it pulls off of raw PRISM data received under 702 into its other databases. While this has to be targeted off a foreign target, that surely includes a lot of US person data, and metadata including Internet based calls, photos, as well as emails. CIA does a lot of metadata queries for other entities (other IC agencies? foreign partners? who knows!), and they don't count it, so they are clearly doing a lot of it.

FBI

As far as we know, FBI does not have a true "bulk" dragnet, sucking up all the phone or Internet records for the US or foreign switches. But it surely has fairly massive metadata repositories itself.

Until 2006, it did, however, have something almost identical to what we understand Hemisphere to be, all the major telecoms, sitting onsite, ready to do sophisticated analysis of numbers offered up on a post-it note, with legal process to follow (maybe) if anything nifty got turned over. Under this program, AT&T offered some bells and whistles, included "communities of interest" that included at least one hop. That all started to get moved

offsite in 2006, when DOJ's IG pointed out that it didn't comply with the law, but all the telecoms originally contracted (AT&T and the companies that now comprise Verizon, at least), remained on contract to provide those services albeit offsite for a few years. In 2009, one of the telecoms (which is likely part or all of Verizon) pulled out, meaning it no longer has a contract to provide records in response to NSLs and other process in the form the FBI pays it to.

FBI also would have a database of the records it has collected using NSLs and subpoenas (I'll go look up the name shortly), going back decades. Plus, FBI, like CIA, can "upload or transfer some or all" of the metadata that it pulls off of raw PRISM data received under 702. So FBI has its own bulky database, but all of the data in it *should* have come in in relatively intentional if not targeted fashion. What FBI does have *should* date back much longer than NSA's Section 215 database (30 years for national security data) and, under the new Section 309 restrictions on EO 12333 data, even NSA's larger dragnet. On top of that, AT&T still provides 7 bells and whistles that are secret and that go beyond a plain language definition of what they should turn over in response to an NSL under ECPA (which probably parallel what we see going on in Hemisphere). In its Section 215 report, PCLOB was quite clear that FBI almost always got the information that could have come out of the Section 215 dragnet via NSLs and its other authorities, so it seems to be doing quite well obtaining what it needs without collecting all the data everywhere, though there are abundant reasons to worry that the control functions in FBI's bulky databases are craptastic compared to what NSA must follow.

IS THERE A PROGRAMMATIC STINGRAY?

The NYT yesterday had a story on the secrecy surrounding Stingrays including these admissions from an FBI affidavit to explain the secrecy.

> A fuller explanation of the F.B.I.'s position is provided in two publicly sworn affidavits about StingRay, including one filed in 2014 in Virginia. In the affidavit, a supervisory special agent, Bradley S. Morrison, said disclosure of the technology's specifications would let criminals, including terrorists, "thwart the use of this technology."
>
> "Disclosure of even minor details" could harm law enforcement, he said, by letting "adversaries" put together the pieces of the technology like assembling a "jigsaw puzzle." He said the F.B.I. had entered into the nondisclosure agreements with local authorities for those reasons. In addition, he said, the technology is related to homeland security and is therefore subject to federal control.
>
> In a second affidavit, given in 2011, the same special agent acknowledged that the device could gather identifying information from phones of bystanders. Such data "from all wireless devices in the immediate area of the F.B.I. device that subscribe to a particular provider may be incidentally recorded, including those of innocent, nontarget devices."
>
> But, he added, that information is purged to ensure privacy rights.

In response, a bunch of smart people had an

interesting conversation today about why the government is so secretive about them (start at this tweet).

My wildarseguess is that they're hiding some kind of programmatic Stingray program. I think so for three reasons:

- Any programmatic Stingray program would (have) been hidden by carve-outs in USA Freedom Act's transparency provisions
- At least one of the liberated non-disclosure agreements suggests ongoing obligations between localities and the FBI
- FISC appears to have permitted more expansive versions of criminal PRTT programs

In past legislative debates the Intelligence Community revealed secret programs by defending them

I believe one of the best ways to see vague outlines of undisclosed domestic surveillance is to watch where the Intelligence Community is most intransigent on legislation.

When Michaels Mukasey and McConnell wrote a transparently bullshit response to a Russ Feingold effort to segregate incidentally collected US person data under FISA Amendments Act in early 2008, I guessed they were doing back door searches of that data. 4 and 5 years later (with the report on the reauthorization and Snowden disclosures, respectively), that was

proven correct.

When the IC repeatedly and successfully defeated efforts to require some real connection between a target and the records collected using Section 215 in 2009 all while boasting they had used it in the Najibullah Zazi investigation, I guessed they were using Section 215 to collect bulky data. I even guessed that they had migrated Bush's illegal wiretap program to Section 215 and PRTT (though a former prosecutor friend soon dissuaded me from pushing my PRTT analysis because, she pointed out, there was no way in hell PRTT could authorize a dragnet).

There were 3 parts of the USA Freedom Act which struck me as particularly notable in the same way. First, the government's insistence on expanding the chaining process to include "connections" in addition to contacts; I strongly believe that indicates they ask cell companies to match up the various identities with a particular handset.

Then there were two kinds of programmatic collection that would not only not be shut down by the prohibition on bulk collection in the bill, but which were specifically excluded from individualized transparency reporting (in addition to back door searches and upstream domestic collection, but we already knew about both of those), because transparency in the bill only covered "communications." The first is any kind of dragnet tied to a non-communication corporate name, such as a financial dragnet or hotel records. See this post for an explanation. USAF would not require individualized reporting on this collection at all. Particularly given that the bill would permit using corporate names as identifiers and would exclude that from transparency, I think reasonable people should assume that kind of bulky collection would continue unabated.

More interesting, though, the transparency provisions also appear to exempt tracking device collection from individualized reporting, because those aren't considered "communications"

from individualized transparency reporting (I believe it would also exempt cloud data but I don't understand what this is yet). I don't think the government could use "Harris Corporation" as a identifier (they wouldn't need to anyway, because the FBI would be using the tool not collecting all of Harris' data). But they could collect the tracking data on 310 million people and only need to report targets (which currently number in the hundreds, though there already is some gaming of the required US person target reporting).

Like a Stingray, which looks for one phone, but obtains the records of everyone in a cell area.

Which is why I love this quote from the NYT article:

> Christopher Allen, an F.B.I. spokesman, said "location information is a vital component" of law enforcement. The agency, he said, "does not keep repositories of cell tower data for any purpose other than in connection with a specific investigation."

The government currently collects phone records of some significant subset of 310 million Americans for the purposes of "specific investigations." It's just that they consider enterprise investigations to be "specific" and therefore every American to be "relevant." The same may well apply to location data.

FBI's non-disclosure agreement(s) suggests ongoing cooperation between local and federal law enforcement

We've already seen plenty of evidence that local law enforcement retain their ties and obligations to federal law enforcement, largely in the demands the Marshal service puts on secrecy.

But as I lay out in this post, that seems to involve ongoing cooperation using the Stingray. An NDA liberated in MN specifically requires deconfliction of missions, indicating that multiple entities would use one Stingray at once.

That all seems to suggest a key part of this top-down hierarchical non-disclosure requirement involves that kind of mission-sharing.

Which is another way of saying that FBI probably relies on these local Stingrays.

FISC appears to permit more expansive PRTT programs than in criminal context

In this post and this one, I showed that the FISC-authorized use of PRTT relates the criminal context but may not be bound by it. That's significant, because we know where the government has obtained permission for Stingray use in the criminal context, they've often relied on PRTT.

In both the use of combined PRTT/215 orders to get location data and in the collection of Post-Cut Through Dialed Digits, FISC has reconsidered PRTT orders after magistrates challenged similar criminal uses. At least in the latter example, FISC permitted FBI to continue a more expansive collection even after it was prohibited in the criminal context, requiring only that FBI comply with Fourth Amendment protections using minimization (as I'll show when I finally write up the remainder of the FISC opinions, this practice has early foundation in other FISC applications).

> What becomes clear reviewing the public records (these reports say this explicitly) is that the 2002 DOJ directive against retaining PCTDD applies to the criminal context, not the FISA context. When judges started challenging FBI's authority to retain

> PCTDD that might include content under criminal authorities, FBI fought for and won the authority to continue to treat PCTDD using minimization procedures, not deletion. And even the standard for retention of PCTDD that counts as content permits the affirmative investigative use of incidentally collected PCTDD that constitutes content in cases of "harm to the national security."
>
> Whateverthefuck that is.
>
> Which is, I guess, how FBI still has 7 uses of PCTDD, including one new one since 2008.

In other words, the Stingray use we see glimpses of in the criminal and fugitive context may be far short of what FISC has permitted in the national security context, if it tracks other practice. And accused terrorists (or spies) would not get notice of any such PRTT use so long as it wasn't entered into a criminal proceeding (there have been several instances where the government has seemed to suggest PRTT was used, but evidence from it not entered into evidence).

All of this, of course, is speculative.

But there's some reason the government is insisting on its expansive NDAs even while more and more people are discussing them. Hiding a more comprehensive program targeted at national security targets (terrorists and spies) might explain why the government is increasingly willing to forgo prosecutions of alleged criminals to keep what they're doing with dragnets secret.

Update: Meanwhile, in NY, a judge has ordered the Erie County Sheriff to come clean on its Stingray use.

SONY, HACKED: IT'S NOT ONE MASSIVE BREACH – IT'S MORE THAN 50 BREACHES IN 15 YEARS

Ever try to follow an evolving story in which the cascade of trouble grew so big and moved so fast it was like trying to stay ahead of a pyroclastic flow?

That's what it's like keeping up with emerging reports about the massive cyber attack on Sony. (Granted, it's nothing like the torture report, but Hollywood has a way of making the story spin harder when it's about them.)

The *second* most ridiculous part of the Sony hack story is the way in which the entertainment industry has studiously avoided criticizing those most responsible for data security.

In late November, when the hacker(s) self-identified as "Guardians of Peace" made threats across Sony Pictures' computer network before releasing digital film content, members of the entertainment industry were quick to revile pirates they believed were intent on stealing and distributing digital film content.

When reports emerged implicating North Korea as the alleged source of the hack, the industry backpedaled away from their outrage over piracy, mumbling instead about hackers.

The industry's insiders shifted gears once again it was revealed that Sony's passwords were in a

password-protected file, and the password to this file was ‘password.‘

At this juncture you’d think Sony’s employees and contractors — whose Social Security numbers, addresses, emails, and other sensitive information had been exposed — would demand a corporate-wide purge of IT department and Sony executives.

You’d think that anyone affiliated with Sony, whose past and future business dealings might also be exposed would similarly demand expulsion of the incompetents who couldn’t find OPSEC if it was tattooed on their asses. Or perhaps investors and analysts would descend upon the corporation with pitchforks and torches, demanding heads on pikes because of teh stoopid.

Nope.

Instead the industry has been tsk-tsking about the massive breach, all the while rummaging through the equivalent of Sony Pictures’ wide-open lingerie drawer, looking for industry intelligence. Reporting by entertainment industry news outlets has focused almost solely on the content of emails between executives.

But the *first* most ridiculous part of this massive assault on Sony is that Sony has been hacked more than 50 times in the last 15 years.

Yes. That’s More Than Fifty.

Inside Fifteen Years.

Granted, this is not just Sony’s film studio business, but Sony Corporation, the Japanese conglomerate which includes Sony Pictures Entertainment, and Sony Computer Entertainment (the parent of PlayStation products). The cyber attacks have focused on these two entities, more so than Sony’s manufacturing and finance subsidiaries. But one would think that management at the top of the holding company structure would eventually demand ALL subsidiaries institute a baseline cyber security overhaul.

The first hack was in 1999, when a Sony website was defaced. This was a recurring theme for several years – 52 times websites across the Sony Group were defaced, between 1999 and early 2011.

Two times during the same period, Sony Computer Entertainment's PlayStation PS3 games or accounts were hacked; customer credit card numbers were compromised, and SonyRewards program was breached – that's a total of 56 attacks inside twelve years.

The attacks exploded after the first quarter of 2011, amounting to a total of 21 in that banner year alone. The worst attack in terms of scale affected 77 million PlayStation Network (PSN) users' accounts. It was only the first multi-million account breach in 2011, however, and PSN was offline for 24 days due to another attack.

Though far fewer in number, cyber attacks since 2011 have been costly to Sony subsidiaries. The entire catalog of Michael Jackson's songs was stolen sometime in 2011, but acknowledged in March 2012. In November 2013, Sony PSN notices unusual activity and resets passwords for an unspecified number of PSN user accounts.

The massive cyber attack in November was not the only one this year. In August, a group calling themselves the "Lizard Squad" spawned a distributed denial of service focused on PSN; at the same time, a bomb threat had been called in, causing diversion of the plane on which Sony's president of its online entertainment subsidiary was traveling.

In February 2014, credentials for one or more Sony Pictures Entertainment servers were obtained by hackers and used to upload malware. Sony did not disclose the attack to the public as the breach appears to have occurred in Brazil, where no law requires such a disclosure. This may have been the initial vector of infection and attack by the Guardians of Peace, culminating in the November data breach, though it is not clear based on the information

available to date.

What is clear from Sony subsidiaries' cyber security history is that Sony has a massive, holding company-wide problem with operations security, and the problem is deeply embedded in its culture if attacks have not been stemmed over the last 15 years.

It is also clear that the entertainment industry – beyond the disturbing attributes like racism and sexism revealed by materials exposed in Sony's breached records – shares an equally troubled attitude toward operations security.

This seems particularly odd for an industry that relies on intellectual property and digital distribution. The industry may complain heartily about piracy, but they are not prepared to lock the doors against incursions, preferring instead to buy influence – through its trade association MPAA – with politicians and law enforcement rather than actually protect their creative works and their employees.

Reaction among the other major film studios has been tepid to altogether mute. One report said Twenty-First Century Fox was considering a request for employees to change their passwords.

(Oh, such bold leadership with aggressive implementation of heightened security efforts…)

But the proof is in the pudding. Hackmageddon's aggregate reports of cyber attacks on major firms over the last handful of years reveals that of the major studios, only Warner Brothers and FOX were attacked a couple of times each, and the breaches were relatively small compared to the scale of 2011 aand 2014 attacks on Sony.

Putting aside the issue of lousy OPSEC, one might well ask why Sony? The theory that North Korea is behind this latest massive breach is split among the cyber security community. NK's complaint filed with the United Nations about Sony's scheduled release of the comedy, The Interview, poking fun at Kim Jong-un supplies a motive. But the complaint letter was filed in

June, and the two known breaches from February and November this year don't align well with that time frame. NK was cryptic in response to early questions about its responsibility; it later denied responsibility.

Some speculate the attack was cyber crime, intended to extort money out of the corporation based on the threat sent to executives on November 21st, before the hackers released Sony's data. The demand read, "We've got great damage by Sony Pictures. The compensation for it, monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as a whole."

A payout was not and is not feasible, as any sizable cash payout would necessarily require the sign-off of board of directors, and they in turn would be held accountable by shareholders. It's simply not a logical, workable scenario.

It's not impossible the breach was the work of hacktivists. Motives for such an attack are not clear, however. The messy clues to the hack's origins fit more closely with reasons of vengeance, though any rationale beyond NK's anger about The Interview is murky.

No matter the origins of the hack, the beneficiaries of the attack are the competing major studios. Sony Pictures' ~11% share of the movie industry may fall if confidence in the studio does not improve. Investors shorting Sony may also benefit from a recent downturn in Sony's ADR price.

The losers are the employees and larger creative community dependent upon Sony's business. They deserved better protection that even simple changes to security would have afforded them.

And of course the public deserved better than the questionable testimony the president of Sony Network Entertainment International Tim Schaaf gave before Congress back in June 2011, after the enormous breaches of PSN's users' data that spring:

> “Sony Network Entertainment and Sony Online Entertainment have always made concerted and substantial efforts to maintain and improve their data security systems.”

Ri-ight.

[graphic: Merrill College of Journalism via Flickr]

NSA ONLY FINDS 59% OF ITS TARGETING OF US PERSONS

This will be a minor point, but one that should be made.

The Privacies and Civil Liberties Oversight Board report on Section 702 included this little detail:

> In 2013, the DOJ undertook a review designed to assess how often the foreignness determinations that the NSA made under the targeting procedures as described above turned out to be wrong – i.e., how often the NSA tasked a selector and subsequently realized after receiving collection from the provider that a user of the tasked selector was either a U.S. person or was located in the United States. The DOJ reviewed one year of data and determined *that 0.4% of NSA’s targeting decisions resulted in the tasking of a selector that, as of the date of tasking, had a user in the United States or who was a U.S. person*. As is discussed in further detail below, data from such taskings in most instances must be purged. The purpose of

> the review was to identify how often the NSA's foreignness determinations proved to be incorrect. Therefore, the DOJ's percentage does not include instances where the NSA correctly determined that a target was located outside the United States, but post-tasking, the target subsequently traveled to the United States.

0.4% of NSA's targeting decisions falsely determine someone is a foreigner who is in fact a US person.

That's a pretty low amount. Though based on ODNI's number — showing 89,138 people were targeted in 2013 — that means 356 US persons get wrongly targeted each year. Again, still not a huge number, but it compares rather interestingly with the 1,144 people targeted under FISA each year. Those wrongly targeted under Section 702 actually make up 24% of those targeted in a year.

Just as interesting is comparing the NSA's internal audit (see page 6) with DOJ's results. For a period presumably covering some of the same time period, NSA discovered 20 US persons tasked (for some reason there was a big increase in this number for the last quarter of the report) and 191 incidences of "other inadvertent" tasking violations, which are described as, "situations where targets were believed to be foreign but who later turn out to be U.S. persons *and other incidents that do not fit into the previously identified categories*" (my emphasis). Not all of those 191 incidents should be counted as wrongly targeted US persons — the description includes other inadvertent targeting. But even counting them all as such, that means NSA only found 211 of the potential wrongly targeted US persons in a year, while DOJ found 356.

Again, in a country of 310 million people, these numbers are small, particularly as compared to the collection of US person communications under

upstream collection, which is thousands of times higher.

But it does say that NSA's internal reviews don't find all the Americans who get wrongly targeted.

Correction: I originally mistranscribed DOJ's number as .o4%—though I had calculated using .4%.

WORKING THREAD, PCLOB REPORT

The pre-release PCLOB report on Section 702 is here. This will be a working thread.

PDF 16: First recommendation is to include more enunciation of foreign intel purpose. This was actually a Snowden revelation the govt poo pooed.

PDF 17: Recommends new limits on non-FI criminal use of FBI back door searches, and some better tracking of it (surprised that's not stronger!). Also recommends new documentation for NSA, CIA back door queries. Must mean CIA is a problem.

PDF 17: Recommends FISC get the "rules" NSA uses. That suggests there may be some differences between what the govt does and what it tells FISC it does.

PDF 17: Recommends better assessment of filtering for upstream to leave out USP data. John Bates was skeptical there wasn't better tech too.

PDF 18: Suggestion there are more types of upstream collection than there needs to be.

PDF 27 fn 56: Notes some room in the definition of Foreign Intelligence.

PDF 30: Note how PCLOB deals with issues of

scope.

PDF 34: Note the discussion of due diligence. Due diligence problems amount for about 9% of NSA violations.

PDF 34-35: This must be a response to violations reported by Risen and Lichtblau, and is probably one of the things referred to in NSA's review of its own COINTELPRO like problems.

> In a still-classified 2009 opinion, the FISC held that the judicial review requirements regarding the targeting and minimization procedures required that the FISC be fully informed of every incident of noncompliance with those procedures. In the 2009 opinion, the court analyzed whether several errors in applying the targeting and minimization procedures that had been reported to the court undermined either the court's statutory or constitutional analysis. (The court concluded that they did not.)

PDF 39: NSA gets all PRISM collection, and it goes from there to CIA and FBI. CIA and FBI get only PRISM data.

PDF 42: Another FISC opinion to be released.

> In a still-classified September 2008 opinion, the FISC agreed with the government's conclusion that the government's target when it acquires an "about" communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector.

PDF 43: This sounds like a lot of about collection is of forwarded emails.

> There are technical reasons why "about" collection is necessary to acquire even some communications that are "to" and "from" a tasked selector. In addition,

> some types of “about” communications actually involve Internet activity of the targeted person.138 The NSA cannot, however, distinguish in an automated fashion between “about” communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets.139

PDF 45: I’ll have to check but some of these cites to Bates may be to still redacted sections.

[Headed to bed—will finish my read in the AM]

PDF 47: One thing PCLOB doesn’t explain is if the FBI and CIA targeting takes place at NSA or at those agencies. In the past, it had been the former.

PDF 49: .4% o f targeting ends up getting an American.

PDF 55: NSA shares technical data for collection avoidance purposes. This sounds like the defeat list in the phone dragnet, and like that, seems tailored not just for protecting USPs generally, but sensitive communications (like those of MoCs) more specifically.

PDF 57: This was implicit in some of the docs released by Snowden, but the govt now tags Section 702 data, as they do Section 215, so as to ensure it gets the heightened treatment provided by the law.

PDF 58: PCLOB says, “The NSA’s core access and training requirements are found in the NSA’s targeting procedures, which have not been released to the public.” But they have, by Edward Snowden. And there are not explicit training requirements in those, which were released in 2009, just the general ones on page 7. It’s possible those have been updated, but from a bureaucratic perspective, that language doesn’t accomplish what PCLOB says it does. The

FBI training is “mandatory online” which from everything we’ve seen means shitty-ass.

PDF 59: PCLOB addresses NCTC’s minimization procedures (and seems to confirm that no one besides NCTC has gotten direct access to 702 information), which I wrote about when the Semiannual Compliance report was released last August. The NCTC has access to FBI databases, and their MPs require them not to use purely law enforcement information.

PDF 60: Note the agencies can use key words or phrases when they’re querying collected 702 data.

PDF 60: PCLOB confirms that NSA has its 702 data mixed in with other data, with the tags to limit access to those with training.

PDF 61: FBI can conduct federated queries. That results exist shows up even if they don’t have the training for Section 702.

> At the FBI, an agent or analyst who conducts a “federated query” across multiple databases, but who does not have Section 702 training, would not receive the Section 702–acquired information as the result of a query. The agent or analyst would, however, be notified in their query results of the fact that there is responsive information to their query in a database containing unminimized Section 702–acquired information to which he or she does not have access. In order to gain access to this information, the analyst or agent would need to either take the requisite training to gain access to the Section 702 information or contact a fellow agent or analyst who had the requisite training to determine whether the responsive results can be disseminated pursuant to the minimization procedures.

PDF 61-62: NSA can query upstream telephony

collection (as distinct from upstream Internet collection). Remember telephony identifiers have been going up recently.

PDF 62: PCLOB cites the October 2011 minimization procedures for claim that NSA can only query w/additional justification. But at that point, those rules were not in place. That raises questions about how closely they reviewed this aspect of things (though likely arises from their desire to cite only declassified documents).

PDF 62: PCLOB says Section 105 (traditional FISA) and Section 704 (overseas stored content) may be queried. This introduces an apparent discontinuity in current rules, because in the most recent primary orders, only Section 105 identifiers may be automatically RAS-approved. Note the absence of 703 here; NSA doesn't use that for some reason.

PDF 63: Provides more information on CIA's back door searches, which seem to me especially problematic. The metadata searches aren't tracked, and the CIA can then use that to argue for getting the content.

PDF 64: FBI searches on its FISA content when it starts new NatSec investigations. Most people who do NatSec investigations can access this content. FBI relies on anecdote alone to claim that other criminal investigations would not return FISA information.

PDF 65: Here's what PCLOB says about FBI's retention policies.

> The FBI's minimization procedures alone distinguish between acquired data that have not been reviewed and those that have not been determined to meet the retention standard. As with the NSA and CIA, Section 702–acquired communications that have not been reviewed must be aged off FBI systems no later than five years after the expiration of the Section 702 certifications under which the data was acquired. Data that was reviewed but not

> yet determined to meet the retention standard in the FBI minimization procedures may be kept for a longer retention period subject to additional access controls.

Prior to this, though, it speaks of "U.S. person information that meets the standard for permanent retention" (though that's apparently not an FBI specific thing). That suggests, first of all, that FBI may be searching in unsearched content up to 6 years after it was collected, but that some of this gets kept for all time, whether or not someone is charged. Note, while the PCLOB report discusses Riley v. CA, it doesn't appear to discuss the 2nd circuit decision on searching of previously collected data.

PDF 67: PCLOB confirms what was already obvious: not much USP inclusive info gets purged upon identification because foreign intelligence.

> The NSA's general counsel, however, clarified that it is often "difficult to determine the foreign intelligence value of any particular piece of information."268 An NSA analyst would need to determine not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need. Thus, in practice, this requirement rarely results in actual purging of data.

And none does at CIA and FBI.

> Neither the CIA nor FBI's minimization procedures have comparable requirements that a communication containing U.S. person information be purged upon recognition that the communication contains no foreign intelligence

> information; instead the CIA and FBI rely solely upon the overall age-off requirements found in their minimization procedures.

PDF 68: NSA will keep a communication if it's evidence of a crime and it has *or will* send it to a federal LE agency. Note, other things had specified FBI here. This suggest DEA or other Fed LE agencies (Secret Service covers cybercrime, for example) may get the data instead. This passage also explicitly admits that encrypted comms get saved indefinitely.

PDF 68: PCLOB does not note that EO 12333 was changed in 2008 to make FISA pre-empt 12333, whereas previously they both applied. So its language about EO 12333 applying is moot.

PDF 68: Once CIA "minimizes" FISA comms (which does not necessarily result in removing USP data), people who have not been trained in FISA can access it.

PDF 69: FBI is supposed to keep stuff that is exculpatory.

PDF 69: PCLOB doesn't mention that the government hadn't been complying with notice requirements.

PDF 71: PCLOB says this about FBI dissemination.

> The FBI's minimization procedures permit the FBI to disseminate Section 702–acquired U.S. person information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information. Disseminations concerning the national defense or security of the United States or the conduct of foreign affairs of the United States are permitted to identify U.S. persons only if necessary to understand the foreign intelligence information or to assess its importance. The FBI is also permitted to disseminate U.S. person

> information that reasonably appears to be evidence of a crime to law enforcement authorities. The FBI's minimization procedures incorporate certain guidelines, already otherwise applicable to the FBI, regarding the dissemination of information to foreign governments.

Note that while it does acknowledge that FBI sometimes shares with foreign governments (so does CIA and NSA, which it doesn't discus) it also doesn't acknowledge that FBI has liberal sharing rules for dissemination to local law enforcement and things like fusion centers.

PDF 72: PCLOB makes much of NSA's Director of Civil LIberties and Privacy.

> The NSA appointed its first Director of Civil Liberties and Privacy while the Board was conducting its review of the Section 702 program. The Director's office is not, as of yet, involved in periodic Section 702 programmatic reviews. The Director's first public report, however, was issued in April 2014 and described in an unclassified manner aspects of the NSA's implementation of the Section 702 program.

It also relies heavily on the Director's report ,which I've noted reads like propaganda. It does this even while ignoring things in the public domain, like the leaked targeting procedures. This harms the credibility of this report.

PDF 72: It would have been really helpful for PCLOB to note how many CIA and FBI people access FISA data at NSA.

PDF 78: CIA's querying of 702 metadata is a black hole.

> At the CIA, the NSD/ODNI team reviews the CIA's querying, retention, and

> dissemination of Section 702–acquired data.332 The NSD/ODNI team evaluates all of the required written justifications for use of a U.S. person identifier (or any other query term intended to return information about a particular U.S. person) to query Section 702–acquired content.333 Metadata queries are not reviewed

ODF 80: This discussion of IG reports is wholly inadequate.

> Section 702 also authorizes inspectors general of agencies that acquire data pursuant to Section 702 to conduct reviews of the Section 702 program.347 The inspectors general are authorized to evaluate the agencies compliance with the targeting procedures, minimization procedures, and Attorney General Guidelines.348 Any such reviews are required to contain an accounting of the number of disseminated reports containing U.S. person identities, the number of instances those identities were unmasked, and the number of targets that were subsequently determined to be located in the United States.349 The results of these reviews must be provided to the Attorney General, Director of National Intelligence, FISC, and the Congressional Committees.350 The NSA and DOJ351 Inspectors General have conducted reviews under this provision. The reports of these reviews have not been declassified.

At a minimum, it should discuss that NSA's IG has been late with crucial reports. It should explain how many reports have been done, and by which IGs.

PDF 82: This language is why it is so egregious that PCLOB doesn't mention DOJ has not complied with notice to defendant requirements.

> These internal and external compliance programs have not to date identified any intentional attempts to circumvent or violate the procedures or the statutory requirements,

PDF 83: This violation shows why tagging data is not sufficient to protect against illegal searches.

> NSA has reported instances in which the NSA analysts conducted queries of Section 702–acquired data using U.S. person identifiers without receiving the proper approvals because the analyst either did not realize that the NSA knew the identifier to be used by a U.S. person or the analyst mistakenly queried Section 702–acquired data after receiving approvals to use a U.S. person identifier to query other non-Section 702–acquired data

PDF 83: The Semiannual Compliance report makes clear this is a telecom-side error, but PCLOB makes no mention of that.

> The government has also disclosed that both changes in how communications transit the telecommunications system and design flaws in the systems the government uses to acquire such communications can, and have, resulted in the acquisition of data beyond what was authorized by Section 702 program.

PDF 84: Significant compliance problems about which we have heard nothing.

> In an earlier incident, the NSA discovered that its practices for executing purges were substantially incomplete. Modifications to better tag, track, and purge data from the NSA's systems when required were implemented.

> More recently, questions raised by the NSD/ODNI oversight team led to the discovery that post-tasking checks used to identify indications that a target is located in the United States were incomplete or, for some selectors, non-existent for over a year. After this issue was discovered, the relevant systems were modified to correct several errors, efforts were made to identify travel to the United States that had been previously missed (and corresponding purges were conducted), and additional modifications to the agencies' minimization procedures were made to ensure that data acquired while a Section 702 target had traveled to the United States will not be used.

Though the latter case appears to be the real problem underlying what the government has claimed was the roamer problem.

PDF 89: PCLOB admits no one had any way of knowing about upstream collection but then decides it's legal because that may be the only way to target some of this communication.

> The fact that the government engages in such collection is not readily apparent from the face of the statute, nor was collection of information "about" a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act. Indeed, the words "target" and "targeting" are not defined in either the original version of FISA or the FISA Amendments Act despite being used throughout the statute. Some commenters have questioned whether the collection of such "about" communications complies with the statute. We conclude that Section 702 may permissibly be interpreted to allow "about" collection as it is currently conducted.

PDF 93: This will be cited in court documents.

> Outside of this fundamental core, certain aspects of the Section 702 program push the entire program close to the line of constitutional reasonableness.

PDF 97: This tension underlies everything.

> Additional consideration is due to the fact that the executive branch, acting under Section 702, is not exercising its Article II power unilaterally, but rather is implementing a statutory scheme enacted by Congress after public deliberation regarding the proper balance between the imperatives of privacy and national security. By establishing a statutory framework for surveillance conducted within the United States but exclusively targeting overseas foreigners, subject to certain limits and oversight mechanisms, "Congress sought to accommodate and advance both the government's interest in pursuing legitimate intelligence activity and the individual's interest in freedom from improper government intrusion."423 The framework of Section 702, moreover, includes a role for the judiciary in ensuring compliance with statutory and constitutional limits, albeit a more circumscribed role than the approval of individual surveillance requests. Where, as here, "the powers of all three branches of government — in short, the whole of federal authority" — are involved in establishing and monitoring the parameters of an intelligence-gathering activity, the Fourth Amendment calls for a different calculus than when the executive branch acts alone.424

PDF 103: PCLOB deals with foreigners targeted

starting here and suggests it will return to the issue on an analysis of POTUS' PPD-28, released in January.

> The President's recent initiative under Presidential Policy Directive 28 on Signals Intelligence ("PPD-28")439 will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws. Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

PDF 104: PCLOB claims,

Thus, use of Section 702 collection for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion, would violate Section 1806.

Yet we've already seen PCLOB to use Section 702 (in part, along with EO 12333 collection) to combat dissent, when it collected on US critics' online sex habits to discredit them. And I believe that Glenn Greenwald's upcoming Intercept report will have more of this.

PDF 104: PCLOB mentions this as a protection.

> Further, FISA provides special protections in connection with legal proceedings, under which an aggrieved person — a term that includes non-U.S. persons — is required to be notified prior to the disclosure or use of any Section 702–related information in any federal or state court.447 The aggrieved person may then move to suppress the evidence on the grounds that it was unlawfully acquired and/or was not in conformity with the authorizing Section

> 702 certification.448 Determinations regarding whether the Section 702 acquisition was lawful and authorized are made by a United States District Court, which has the authority to suppress any evidence that was unlawfully obtained or derived.449

But then fails to mention that DOJ has failed to comply with this requirement.

PDF 109: Because PCLOB's mandate only covers CT, it doesn't talk about other uses, which would be more problematic to privacy. DiFi's awful cyber sharing bill would extend PCLOB's mandate into cyber.

> Because the oversight mandate of the Board extends only to those measures taken to protect the nation from terrorism, our focus in this section is limited to the counterterrorism value of the Section 702 program, although the program serves a broader range of foreign intelligence purposes.

PDF 110: I increasingly suspect the government is relying on the lone wolf provision, which probably makes it easier to wiretap Muslims it would not put on white extremists.

> Moreover, when the target of surveillance is a U.S. person, that person must be "knowingly" acting on behalf of a foreign power. *See* 50 U.S.C. § 1801(b)(1), (2). An exception to the requirement that the target be acting on behalf of a foreign power permits a so-called "lone wolf" with no apparent connection to a foreign power to be targeted, if there is probable cause that the person is engaged in international terrorism or proliferation of weapons of mass destruction. *See* 50 U.S.C. §§ 1801(b)(1)(C), (D), 1805(a)(2)(A).

PDF 112: This entire discussion is fully of subtext.

> The government also conducts foreign intelligence surveillance outside of the United States against non-U.S. persons under the authority of Executive Order 12333. In some instances, this surveillance can capture the same communications that the government obtains within the United States through Section 702. And because this collection takes place outside the United States, it is not restricted by the detailed rules of FISA outlined above.471 Nevertheless, Section 702 offers advantages over Executive Order 12333 with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. In addition, acquiring communications with the compelled assistance of U.S. companies allows service providers and the government to manage the manner in which the collection occurs. By helping to prevent incidents of overcollection and swiftly remedy problems that do occur, this arrangement can benefit the privacy of people whose communications are at risk of being acquired mistakenly.
>
> 471 FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes.

> *See* 50 U.S.C. §§ 1801(f), 1881c.

PCLOB doesn't admit what we all know: that in some cases (under the Muscular program) NSA is getting precisely the stame stuff available under PRISM. Thus, it doesn't have to offer any explanation for this, which citizens (and Google and Yahoo) deserve. Curiously PCLOB notes that collecting in the US can protect sources and methods. But I increasingly suspect they do some of this to avoid having to share details with the providers.

And the discussion of the limits on surveillance overseas is telling. It emphasizes the particularly of people—because of course the US collects plenty of bulk data including US person data. And the radio example is why, in spirit, collection of US person communications should be prohibited.

PDF 113: PCLOB mentions Khalid Ouazzani and Najibulllah Zazi but doesn't mention DOJ did not comply with the statute on notice with them.

> In one case, for example, the NSA was conducting surveillance under Section 702 of an email address used by an extremist based in Yemen. Through that surveillance, the agency discovered a connection between that extremist and an unknown person in Kansas City, Missouri. The NSA passed this information to the FBI, which identified the unknown person, Khalid Ouazzani, and subsequently discovered that he had connections to U.S.-based Al Qaeda associates, who had previously been part of an abandoned early stage plot to bomb the New York Stock Exchange. All of these individuals eventually pled guilty to providing and attempting to provide material support to Al Qaeda.
>
> [snip]
>
> The NSA passed this information to the FBI, which used a national security

> letter to identify the unknown individual as Najibullah Zazi, located near Denver, Colorado.

PCLOB says in 30 cases, 702 IDed the previously unknown target, but DOJ has only given notice to about 5 people.

PDF 116: PCLOB tries to reassure that it's not using "entity" as a gimmick.

> Although the "persons" who may be targeted under Section 702 include corporations, associations, and entities as well as individuals,475 the government is not exploiting any legal ambiguity by "targeting" an entity like a major international terrorist organization and then engaging in indiscriminate or bulk collection of communications in order to later identify a smaller subset of communications that pertain to the targeted entity. To put it another way, the government is not collecting wide swaths of communications and then combing through them for those that are relevant to terrorism or contain other foreign intelligence

Of course, it has done so in the past, so can't be trusted. Moreover, PCLOB Is very assiduously avoiding discussing cyber attacks, even though that application under 702 is unclassified, which presents different problems here.

PDF 119: PCLOB's bracketing off of "domestic dissent" here is cynical. Anonymous and Occupy are both international movements, as is Wikileaks. Anon and WikiLeaks are known surveillance targets.

> Because it disallows *comprehensive* monitoring of any U.S. person, and prohibits deliberately acquiring even a single communication that is known to be solely among people located within the

> United States, the program would serve as a relatively poor vehicle to repress domestic dissent, monitor American political activists, or engage in other politically motivated abuses of the sort that came to light in the 1970s and prompted the enactment of FISA.

PDF 120: This is one of the sections where PCLOB uses CT as a dodge to hide how problematic a lot of incidental collection is. Because it's "the point" of CT 702 does not make it okay in what is deemed espionage (like WikiLeaks).

PDF 121: The numbers of 702 targets are, as compared with 2011's 250 million internet communications "significantly higher." Is there any rational reason this couldn't be declassified?

PDF 123: PCLOB told us that NSA now collects substantially more than 250 million internet communications. It boasts of a 0.4% incorrect tasking rate. But .4% of even 250 million is 1 million. That, um, not small.

> Available figures suggest that the percentage of instances in which the NSA accidentally targets a U.S. person or someone in the United States is tiny. In 2013, the DOJ reviewed one year of data to determine the percentage of cases in which the NSA's targeting decisions resulted in the "tasking" of a communications identifier that was used by someone in the United States or was a U.S. person. The NSA's error rate, according to this review, was 0.4 percent.491

Admittedly the 250M (which is not substantially higher) doesn't correspond to tasking. Using the 89,000 targets released last week, that says 356 people are inappropriately tasked.

PDF 124: This is a particularly disingenuous response to public reports.

> Initial news articles describing "about" collection may have contributed to this perception, reporting that the NSA "is searching the contents of vast amounts of Americans' email and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance[.]"498 This belief represents a misunderstanding of a more complex reality. "About" collection takes place exclusively in the NSA's acquisition of Internet communications through its upstream collection process. That is the process whereby the NSA acquires communications as they transit the Internet "backbone" within the United States.

There's nothing wrong about the report (except that it doesn't note the initial scan takes place at telecoms, but the volume is greater than indicated). Savage didn't use "key word" here. It's just that PCLOB is okay with this because it thinks it should continue even if there's not technical way to do it without infringing on US person privacy.

That's especially true given this footnote, on PDF 127:

> The term *"about" communications* was originally devised to describe communications that were "about" the selectors of targeted persons – meaning communications that contained such a selector within the communication. But the term has been used more loosely by officials in a way that suggests these communications are "about" the targeted persons. References to targeted *persons* do not themselves lead to "about" collection; only references to the communications *selectors* of targeted persons lead to "about" collection.

That is, one reason for the confusion is that the government is being dishonest about what it's doing.

PDF 126: Here's how PCLOB spun NSA's refusal to count domestic upstream collection.

> Although the NSA conducted a study in 2011, at the behest of the FISA court, to estimate how many wholly domestic communications it was annually acquiring as a result of collecting "MCTs" (discussed below), the study did not focus on how many domestic communications the NSA may be acquiring due to "about" collection where the communication acquired was not an MCT but rather a single, discrete communication. Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11, n.32. At the urging of the FISA court, the NSA subsequently spent some time examining this question, but ultimately did not provide an estimate, instead explaining to the court the logistical reasons that the chance of acquiring domestic communications in "about" collection "should be smaller – and certainly no greater – than potentially encountering wholly domestic communications within MCTs." *Id*. This statement prompted the FISA court to adopt the assumption that the percentage of wholly domestic communications within the agency's "about" collection might equal the percentage of wholly domestic communications within its collection of "MCTs," leading to an estimate of as many as 46,000 wholly domestic "about" communications acquired each year. *Id*. We do not view this as a particularly valid estimate, because there is no reason to suppose that the number of wholly domestic "about" communications matches the number of wholly domestic MCTs, but the fact remains that the NSA

> cannot say how many domestic "about" communications it may be obtaining each year.

This is ridiculous! The NSA basically refused to do analysis on a small subset of communications to get a real answer. That ought to raise suspicions, not excuses of why Bates' effort to come up with his own estimate fails. Besides, there are a lot of technical reasons to expect the number of completely domestic communications are much higher than the MCT rate.

PDF 126: Here's PCLOB's admission of the huge problem with "about" collection, though it backs off admitting NSA collects on malware (which is known) or Inspire decryption code (which I strongly suspect).

> The more fundamental concern raised by "about" collection is that it permits the government to acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications.509 This practice fundamentally differs from "incidental" collection, discussed above. While incidental collection also permits the government to acquire communications of people about whom it may have had no prior knowledge, that is an inevitable result of the fact that conversations generally involve at least two people: acquiring a target's communications by definition involves acquiring his communications with other people. But no effort is made to acquire those other peoples' communications — the government simply is acquiring the target's communications. In "about" collection, by contrast, the NSA's collection devices can acquire communications to which the target is not a participant, based at times on their contents.510

> Nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. From a legal standpoint, under the Fourth Amendment the government may not, without a warrant, open and read letters sent through the mail in order to acquire those that contain particular information.511 Likewise, the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content.512 And without the ability to engage in inspection of this sort, nothing akin to "about" collection could feasibly occur with respect to such traditional forms of communication.

It then goes onto implicitly admit that its earlier discussion, which suggested that this was often forwarded conversations or somehow still involved the participant, is not right. There are multiple kinds of about which aren't actually email addresses.

PDF 127: This seems to hint at other ways they're using upstream.

> In other instances, a communication may not involve the targeted person, but for various logistical and technological reasons it will almost never involve a person located in the United States.

PDF 130: This is a funny dodge:

> Unlike in PRISM collection, where the government receives communications from the Internet service providers who facilitate them, in upstream collection the NSA obtains what it calls "transactions" that are sent across the backbone of the Internet.

What they don't want to tell you is they're collecting in an inapt spot to get coherent communications. And we're just gonna have to suck it up. Because.

PDF 133: PCLOB is remarkably uncurious about what gets collected in "technical data base" information.

PDF 133: Interesting detail:

> In 2013, for instance, the NSA Director waived the destruction of approximately forty communications (none of which was a wholly domestic communication), involving eight targets, based on a finding that each communication contained significant foreign intelligence information. Neither the CIA nor FBI utilized their waiver provisions in 2013.

That said, PCLOB admits that there are a great many reasons why AGs and DIRNSAs *can* issue waivers, even if they never do. That's a structural problem that should not be overlooked.

PDF 134: Purging never happens.

> Therefore, although a communication must be "destroyed upon recognition" when an NSA analyst recognizes that it involves a U.S. person and determines that it clearly is not relevant to foreign intelligence or evidence of a crime,531 in reality this rarely happens. Nor does such purging occur at the FBI or CIA: although their minimization procedures contain age-off requirements, those procedures do not require the purging of communications upon recognition that they involve U.S. persons but contain no foreign intelligence information.

PDF 134-5: Note that PCLOB doesn't even tell us what they're citing from here, much less the

other things cited?

> No showing or suspicion is required that the U.S. person is engaged in any form of wrongdoing. In recent months, NSA analysts have performed queries using U.S. person identifiers to find information concerning, among other things, "individuals believed to be involved in international terrorism." The CIA and FBI standards for content queries are essentially the same, except that the FBI, given its law enforcement role, is permitted to conduct queries to seek evidence of a crime as well as foreign intelligence information.

PDF 135: I don't think this was really conveyed in the back door search report to Wyden.

> The agency records each term that is approved, though not the number of times any particular term is actually used to query a database.

If the can count how many queries take place with phone dragnet RAS seeds, why can't they count how many queries are made here? The answer is probably because this function is automated in the way they never managed to get the metadata automated.

PDF 136. PCLOB graded the IC's back door search on a curve. I mean, given that these efforts are impossible (PCLOB says "difficult") to evaluate, it means "oversight mechanisms are" NOT "in place."

> As illustrated above, rules and oversight mechanisms are in place to prevent U.S. person queries from being abused for reasons other than searching for foreign intelligence or, in the FBI's case, for evidence of a crime. In pursuit of the agencies' legitimate missions, however, government analysts may use queries to digitally compile the

> entire body of communications that have been incidentally collected under Section 702 that involve a particular U.S. person's email address, telephone number, or other identifier, with the exception that Internet communications acquired through upstream collection may not be queried using U.S. person identifiers.540 In addition, the manner in which the FBI is employing U.S. person queries, while subject to genuine efforts at executive branch oversight, is difficult to evaluate, as is the CIA's use of metadata queries.

Also, when PCLOB says an analyst "may" put all this together, I think evidence suggests that NSA's systems (and probably FBI's) actually does pull up everything. So not "may" but "does."

PDF 137: NSA referred 10 people for crimes, unmasked 10,000 US person identities.

PDF 137: Remember when everyone claimed lawyers weren't being surveilled?

> The NSA also is permitted to use and disseminate U.S. persons' privileged attorney-client communications, subject to approval from its Office of General Counsel, as long as the person is not known to be under criminal indictment in the United States and communicating with an attorney about that matter. *Id*. § 4. The CIA and FBI minimization procedures contain comparable provisions.

PDF 142-43: This seems to be an admission that the FBI minimization procedures (which we've never seen) never told the FISC that Agents pursuing domestic crime are permitted to query Section 702 data.

> Even though FBI analysts and agents who solely work on non–foreign intelligence crimes are not *required* to conduct queries of databases containing Section

> 702 data, they are *permitted* to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI's minimization procedures, and the minimization procedures should be modified to better reflect this actual practice. The Board believes that it is important for accountability and transparency that the minimization procedures provide a clear representation of operational practices. Among other benefits, this improved clarity will better enable the FISA court to assess statutory and constitutional compliance when the minimization procedures are presented to the court for approval with the government's next recertification application.

And it seems to imply that all Agents conducting "foreign" investigations are required to query Section 702.

PDF 143: Note Wald and Medine cite Riley to argue against back door searches (though without noting Roberts' problems with government agency protocols, which they effectively endorse). They don't cite the 2nd Circuit opinion which is even more directly on point.

PDF 144: Brand and Cook seem to be advocating for parallel construction.

> We would also support a requirement of higher-level Justice Department approval, to the extent not already required, before Section 702 information could be used in the investigation or prosecution of a non–foreign intelligence crime (such as in the application for a search warrant or wiretap, in the grand jury, or at trial).

PDF 146: PCLOB slowly coming around to CIA's

metadata searches lacking oversight.

> While U.S. person queries by the NSA and CIA are already subject to rigorous executive branch oversight (with the exception of metadata queries at CIA), supplying this additional information to the FISC could help guide the court by highlighting whether the minimization procedures are being followed and whether changes to those procedures are needed.

PDF 148: I get the feeling the govt hasn’t put rules into minimization procedures precisely to make it hard for government lawyers to get.