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.