THE WEST'S IDEOLOGICAL VACUUM

One point I tried to make in this post on George Orwell's fighting in Spain is that the fight between Bashar al-Assad and ISIS is one that has become an ideological magnet. I was trying to argue that we're offering little by way of positive ideology to combat ISIS, particularly among those most susceptible to its draw.

Two recent commentaries have made related points. This Jocelyne Cesari NYT op-ed on Europe's need to more fully embrace Muslims notes the "collapse" of ideologies in Europe.

> Third, the collapse of all major ideologies in Europe — nationalism, Communism, and liberalism — has left room for new radical options. For some young Europeans, adherence to radical Islam provides a viable alternative ideology, comparable to that of radical leftist groups in the 1970s.

And at the New Yorker, Steve Coll notes that ISIS is the kind of thing that arises when people feel they have no other avenue for security and justice.

> The group's lightning rise is a symptom, however, of deeper instability; a cause of that instability is failed international policy in Iraq and Syria. If the United States is returning to war in the region, one might wish for a more considered vision than Whack-a-Mole against jihadists.
>
> The restoration of human rights in the region first requires a renewed search for a tolerable—and, where possible, tolerant—path to stability. ISIS feasts above all on the suffering of Syria, and that appears to be unending. The war is in its fourth year, with almost two

> hundred thousand dead and nine million displaced, inside the country and out. The caliphate now seated in Raqqa is the sort of dark fantasy that can spring to life when people feel they are bereft of other plausible sources of security and justice.

Though the very terms Coll discusses may betray part of the problem – and the neoliberal ideology Cesari doesn't account for in her piece.

> It is not yet clear that ISIS will endure as a menace. Fast-moving extremist conquerors sometimes have trouble holding their ground. ISIS has promised to govern as effectively as it intimidates, but its talent lies in extortion and ethnic cleansing, not in sanitation and job creation. It is vulnerable to revolt from within.

Conceiving of governance as "job creation" may undersell what a destabilized region is looking for – not to mention ignore what ISIS has done in Syrian areas they control.

> The group also has a surprisingly sophisticated bureaucracy, which typically includes an Islamic court system and a rovingpolice force. In the Syrian town of Manbij, for example, ISIS officials cut off the hands of four robbers. In Raqqa, they forced shops to close for selling poor products in the *suq* (market) as well as regular supermarkets and kebab stands—a move that was likely the work of its Consumer Protection Authority office. ISIS has also whipped individuals for insulting their neighbors, confiscated and destroyed counterfeit medicine, and on multiple occasions summarily executed and crucified individuals for apostasy.

> Members have burned cartons of cigarettes and destroyed shrines andgraves, including the famous Uways al-Qarani shrine in Raqqa.
>
> Beyond these judicial measures, ISIS also invests in public works. In April, for instance, it completeda new *suq* in al-Raqqa for locals to exchange goods. Additionally, the group runs an electricity office that monitors electricity-use levels, installs new power lines, and hosts workshops on how to repair old ones. The militants fix potholes, bus people between the territories they control, rehabilitateblighted medians to make roads more aesthetically pleasing, and operate a post office and *zakat* (almsgiving) office (which the group claims has helped farmers with their harvests). Most importantly for Syrians and Iraqis downriver, ISIS has continued operating the Tishrin dam (renaming it al-Faruq) on the Euphrates River. Through all of these offices and departments, ISIS is able to offer a semblance of stability in unstable and marginalized areas, even if many locals do not like its ideological program.

I'm not saying this is the societal solution the Middle East seeks. But I am saying the US would be wise to understand that ISIS aspires to offer governance, not just brutal war, and it's more likely than, say, AQAP to be able to pull it off.

Meanwhile, Henry Kissinger has an almost plaintive piece calling for a new world order (because the world order he was central in creating is showing signs of cracking) in the WSJ. He ends it with a reaffirmation of purported American exceptionalism, even while he suggests that we must temper our promise of

“individual dignity and participatory governance” in places that need stability within a global order first.

> A world order of states affirming individual dignity and participatory governance, and cooperating internationally in accordance with agreed-upon rules, can be our hope and should be our inspiration. But progress toward it will need to be sustained through a series of intermediary stages.
>
> [snip]
>
> For the U.S., this will require thinking on two seemingly contradictory levels. The celebration of universal principles needs to be paired with recognition of the reality of other regions’ histories, cultures and views of their security. Even as the lessons of challenging decades are examined, the affirmation of America’s exceptional nature must be sustained. History offers no respite to countries that set aside their sense of identity in favor of a seemingly less arduous course. But nor does it assure success for the most elevated convictions in the absence of a comprehensive geopolitical strategy.

But earlier in Kissinger’s piece, he admits that globalization destabilizes political order (even while he overstates the number of winners in the current globalized system).

> The clash between the international economy and the political institutions that ostensibly govern it also weakens the sense of common purpose necessary for world order. The economic system has become global, while the political structure of the world remains based on the nation-state. Economic globalization, in its essence, ignores national frontiers. Foreign policy

> affirms them, even as it seeks to reconcile conflicting national aims or ideals of world order.
>
> This dynamic has produced decades of sustained economic growth punctuated by periodic financial crises of seemingly escalating intensity: in Latin America in the 1980s; in Asia in 1997; in Russia in 1998; in the U.S. in 2001 and again starting in 2007; in Europe after 2010. The winners have few reservations about the system. But the losers—such as those stuck in structural misdesigns, as has been the case with the European Union's southern tier—seek their remedies by solutions that negate, or at least obstruct, the functioning of the global economic system.
>
> The international order thus faces a paradox: Its prosperity is dependent on the success of globalization, but the process produces a political reaction that often works counter to its aspirations.

The rise of ISIS presents several challenges to the US, in my opinion. First, we (and Europe) need to offer something to compete with ISIS' ideology. As loathsome as ISIS' ideology it is, it does aspire to deliver on promises the West increasingly fails to deliver to all.

Part of that, though, requires acknowledging that we do have an ideology — neoliberalism — one that increasingly fails to offer the kind of stability and benefit for all that must offer a better alternative than ISIS (and even more importantly, has failed to provide real nation building in those countries we've destabilized in the Middle East).

ISIS aspires to fill potholes. That's not even something the US can manage (at least not here in MI). That requires a commitment to building society that we've significantly lost of late.

We've been promising for decades that the "free market" will deliver justice everywhere. It seems not to be working. Maybe we need to offer more than that to ideologically combat the dangerous new forces out there?

IS JP MORGAN CRYING CYBERWOLF ABOUT RUSSIA? OR IS MIKE ROGERS?

There was a weird spate of reporting on the cyberthreat to banks last week. Normally, security firms (and occasionally really good tech journalists) report under their own name on such attacks — after all, they have businesses to run! But not the story — first reported by Bloomberg Wednesday evening — that Russia had attacked JP Morgan. At first, these reports appeared to be coming from FBI — given that the FBI investigation served as the lede of the story.

> Russian hackers attacked the U.S. financial system in mid-August, infiltrating and stealing data from JPMorgan Chase & Co. (JPM) and at least one other bank, an incident the FBI is investigating as a possible retaliation for government-sponsored sanctions, according to *two people familiar with the probe*.
>
> The attack resulted in the loss of gigabytes of sensitive data, said the people, who asked not to be identified because the probe is still preliminary.

But over the course of the story — and two more sources introduced with no description beyond

that they had been briefed on the probe – the FBI officially gave no comment.

> The sophistication of the attack and technical indicators extracted from the banks' computers provide some evidence of a government link. Still, the trail is muddy enough that investigators are considering the possibility that it's cyber criminals from Russia or elsewhere in Eastern Europe. Other federal agencies, including the National Security Agency, are now aiding the investigation, *a third person familiar with the probe said*.
>
> [snip]
>
> J. Peter Donald, an FBI spokesman in New York, declined to comment.
>
> [snip]
>
> In at least one of the attacks, the hackers grabbed sensitive data from the files of bank employees, including executives, *according to a fourth person briefed on the probe*, who, like the other individuals with knowledge of the matter, declined to divulge the name of victims other than JPMorgan. Some data related to customers may also have been accessed, the person said.

The NYT's version of the story, published later on Wednesday, also cited a bunch of people described only as "briefed on the continuing investigation."

> A number of United States banks, including JPMorgan Chase and at least four others, were struck by hackers in a series of coordinated attacks this month, according to four people briefed on a continuing investigation into the crimes.
>
> The hackers infiltrated the networks of the banks, siphoning off gigabytes of

> data, including checking and savings account information, in what security experts described as a sophisticated cyberattack.
>
> The motivation and origin of the attacks are not yet clear, according to investigators. The F.B.I. is involved in the investigation, and in the past few weeks a number of security firms have been brought in to conduct forensic studies of the penetrated computer networks.
>
> [snip]
>
> According to two other people briefed on the matter, hackers infiltrated the computer networks of some banks and stole checking and savings account information from clients.

The NYT was able to get the FBI (as well as JP Morgan) on the record.

> "Companies of our size unfortunately experience cyberattacks nearly every day," said Patricia Wexler, a JPMorgan spokeswoman. "We have multiple layers of defense to counteract any threats and constantly monitor fraud levels." Joshua Campbell, an F.B.I. spokesman, said the agency was working with the Secret Service to assess the full scope of attacks. "Combating cyberthreats and criminals remains a top priority for the United States government," he said.

This article (published midday on Thursday) – which casts doubt on the seriousness of the attack – seems to suggest that JPMC leaked to the press, not the FBI.

> "There are no credible threats posed to the financial services sector at this time," [Financial Services Information Sharing and Analysis Center] said in an

> email to its members.
>
> [snip]
>
> JPMorgan had said early on Thursday that it was working with U.S. law enforcement authorities to investigate a possible cyber attack.
>
> The bank provided little information about the suspected attack, declining to say whether it believed hackers had stolen any data or who might be responsible.
>
> “Companies of our size unfortunately experience cyber attacks nearly every day. We have multiple layers of defense to counteract any threats and constantly monitor fraud levels,” it said in a statement.
>
> The FBI had said late on Wednesday that it was looking into media reports on a spate of attacks on U.S. banks, raising concerns that the sector was under siege by sophisticated hackers.
>
> Yet several cyber security experts said that they believe those concerns are overblown.
>
> “Banks are getting attacked every single day. These comments from FS-ISAC and its members indicate that this is not a major new offensive,” said Dave Kennedy, chief executive officer of TrustedSEC LLC, whose clients include several large U.S. banks.

See this Time piece for more reasons why this is probably not the Russian hack it has been pitched as. And the WaPo — in their Wednesday report relying on “officials” — also cast doubt on the claimed motive for the attack, if it is Russia.

But even after the Reuters report casting doubt on the claims about the hack, Bloomberg

continued its reporting — this time suggesting the attack began in June and ended several weeks ago, when previous report said it had started (and this time focusing on JP Morgan alone).

> Hackers burrowed into the databanks of JPMorgan Chase & Co. and deftly dodged one of the world's largest arrays of sophisticated detection systems for months.
>
> The attack, an outline of which was provided by two people familiar with the firm's investigation, started in June at the digital equivalent of JPMorgan's front door, exploiting an overlooked flaw in one of the bank's websites. From there, it quickly developed into any security team's worst nightmare.
>
> The hackers unleashed malicious programs that had been designed to penetrate the corporate network of JPMorgan — the largest U.S. bank, which had vowed two months before the attack began to spend a quarter-billion dollars a year on cybersecurity. With sophisticated tools, the intruders reached deep into the bank's infrastructure, silently siphoning off gigabytes of information, including customer-account data, until mid-August.
>
> [snip]
>
> Evidence of advanced planning and the access to elaborate resources, as well as information provided by the FBI, led some members of the bank's security team to tell outside consultants that they believed the hackers had been aided by the hidden hand of the Russian government, possibly as retribution for U.S.- imposed sanctions.

Bloomberg also made clear that Mike Rogers served as a source of some kind.

> The Federal Bureau of Investigation and other agencies are working on the JPMorgan probe, and House Intelligence Committee Chairman Michael Rogers has been briefed on the bank attacks.

It was all very convenient, blaming Russia (even though investigators hadn't confirmed that's where the attack originated) for scary financial threats.

And then, after several days of all this, Bloomberg published this story, citing the gigabytes of data allegedly taken from JP Morgan, warning that we're all going to have to bail out Jamie Dimon again.

> A worst-case event that destroyed records, drained accounts and froze networks could hurt the economy on the scale of the terrorist attacks of Sept. 11, 2001. The government response, though, might be more akin to that following the 2008 credit meltdown, when the Federal Reserve invoked "unusual and exigent circumstances" to lend billions of dollars.
>
> The government might have little choice but to step in after an attack large enough to threaten the financial system. Federal deposit insurance would apply only if a bank failed, not if hackers drained accounts. The banks would have to tap their reserves and then their private insurance, which wouldn't be enough to cover all claims from a catastrophic event, DeMarco and other industry officials said.
>
> [snip]
>
> Discussions about the government's role in cleaning up after a catastrophic cyber assault have centered on the Terrorism Risk Insurance Act, or TRIA.
>
> [snip]

> The insurance law, enacted after the 2001 attacks, authorizes the government to provide financial support for insurance companies in the wake of terrorism. It is up for renewal this year. Under TRIA, insurers cover a fixed amount of losses from terrorist attacks with the government backstopping additional costs up to $100 billion. The law gives the Treasury secretary broad latitude to invoke the backstop.
>
> In private meetings, Treasury officials have told insurance industry lobbyists that the department would treat cyber-terror like a physical attack under TRIA, said the people involved with the talks, who spoke on condition of anonymity because the discussions were private.

There has been a whole lot of fearmongering over this attack, which insiders doubt happened as billed and/or as attributed to Russia.

But if something like it does happen — gigabytes! — you can be sure Jamie Dimon will stiff us with the bill.

IN A NATION RAVAGED BY BANKSTERS, FBI CAN'T AFFORD THE "LUXURY" OF FRIVOLOUS COUNTERTERRORISM

STINGS

In a JustSecurity post reviewing the same speech that I observed ignored US failures to prevent violent extremism, NYU Professor Samuel Rascoff defends the US use of counterterrorism stings, even in spite of the details revealed by HRW's report on all the problems related to them. David Cole has an excellent response, which deals with many of the problems with Rascoff's argument.

I'd like to dispute a more narrow point Rascoff made when he suggested that, because we have so many fewer trained militants than the Europeans, we "can[] afford" the "luxury" of stings.

> There are now approximately 3,000 European passport holders fighting in Syria and Iraq. In the time that it took Najibullah Zazi to drive from Denver to New York, a fighter could drive from Aleppo to Budapest. What that means is that European officials are relatively more consumed than American counterparts in keeping up with, and tabs on, trained militants. Orchestrating American-style sting operations is, in a sense, a luxury they cannot afford.

The claim is astonishing on its face, in that it suggests that, because we don't have real militants like Europe does, we should engage in the "luxury" of entrapping confused young Muslim men and sending them to expensive decades-long prison terms.

Think a bit more about that notion of "luxury" and the financial choices we make on law enforcement. Here are some numbers taken from two sources: the HRW report (I basically searched on the dollar sign, though this doesn't include every mention of dollars) and today's Treasury settlement with Bank of America for helping 10 drug kingpins launder their money

over a four year period, three years of which constituted "egregious" behavior.

First, HRW reports that FBI spends over $1.3 billion a year on counterterrorism, much of it stings, leaving less than $2 billion for all other investigations.

> More than 40 percent of the FBI's operating budget of $3.3 billion is now devoted to counterterrorism.

That allows the FBI to pay some of its informants and experts hefty sums.

> Beginning in August 2006, the FBI paid Omar $1,500 per week during the investigation. Omar received a total of $240,000 from the FBI. This included: $183,500 in payment unrelated to expenses, and $54,000 for expenses incurred during the investigation including car repair and rent.
>
> [snip]
>
> "Kohlmann is an expert in how to use the Internet, like my 12-year-old. He has found all the bad [stuff] about Islam, and testifies as if what he is reading on the Internet is fact. He was paid around $30,000 to look at websites, documents, and testify."

These informants sometimes promise — but don't deliver — similar hefty sums to the guys they're trying to entrap.

> Forty-five-year-old James Cromitie was struggling to make ends meet when, in 2009, FBI informant Hussain offered him as much as $250,000 to carry out a plot which Hussain—who also went by "Maqsood"—had constructed on his own.
>
> [snip]
>
> The informant proposed to lend Hossain

> $50,000 in cash so long as he paid him back $2,000 monthly until he had paid back $45,000.

Which is particularly important because many of these guys are quite poor (and couldn't even afford to commit the crimes they're accused of).

> At the time he was in contact with the informant and the undercover [agent] he was living at home with his parents in Ashland and he didn't have a car, he didn't have any money and he didn't have a driver's license because he owed $100 and he didn't have $100 to pay off the fine. In various parts of the investigation he didn't have a laptop and he didn't have a cellphone. At one point the informant gave him a cell phone.

And some of these crimes (the very notable exceptions in the HRW report include two material support cases, both of which are close calls on charity designations, but which involved very large sums, $13 million a year in the case of *Holy Land Foundation*) involve relatively minscule sums.

> According to the prosecution, Mirza was the ringleader in collecting around $1,000—provided by the FBI agents and co-defendant Williams—that he handed to a middleman with the intent that it go to families of Taliban fighters.

So one theme of the HRW report is we're spending huge amounts entrapping what are often poor young men in miniscule crimes so taxpayers can pay $29,000 a year to keep them incarcerated for decades.

These are the stakes for what Rascoff calls a "luxury." At a time of self-imposed austerity, these stings are, indeed, a luxury.

Compare that to what happens to Bank of America, which engaged in "egregious" violations of bank reporting requirements for three years (and non-egregious ones for a fourth), thereby helping 10 drug kingpins launder their money. No one will go to jail. Bank of America doesn't even have to admit wrong-doing. Instead, it will have to pay a $16.5 million fine, or just 0.14% of its net income last year.

This settlement came out of a Treasury investigation, not an FBI one.

But when DOJ's Inspector General investigated what FBI did when it was given $196 million between 2009 and 2011 to investigate (penny ante) mortgage fraud, FBI's focus on the issue actually *decreased* (and DOJ lied about its results). When FBI decided to try to investigate mortgage fraud proactively by using undercover operations, like it does terrorism and drugs, its agents just couldn't figure out how to do so (in many cases Agents were never told of the effort), so the effort was dropped.

Banks commits crimes on a far grander scale than most of these sting targets. But FBI throws the big money at its counterterrorism stings, and not the banks leaching our economy of its vitality.

Rascoff accuses HRW's and similar interventions of being one-dimensional.

> [F]or all the important questions about official practices that critics raise, they have tended to ignore some hard questions about the use of stings and the tradeoffs they entail.Instead, their interventions have an exaggerated, one-dimensional quality to them.

But he himself is guilty of his own crime. Because every kid the FBI entraps in a $240,000 sting may represent an actual completed bank crime that will never be investigated. It represents an opportunity cost. The choice is not just sting or no sting or (more accurately,

as David Cole points out) sting or community outreach and cooperation.

Rather, the choice is also between manufacturing crimes to achieve counterterrorism numbers or investigating real financial crimes that are devastating communities.

So long as we fail to see that tradeoff, we fail to address one major source of the economic malaise that fuels other crimes.

Ignoring bank crimes is, truly, something we don't have the luxury of doing. Nevertheless, we continue to choose to go on doing so, even while engaging in these "luxurious" counterterrorism stings that accomplish so little.

WHY CHALLENGE THE WASHINGTON CONSENSUS NOW?

A number of outlets are reporting on the BRICS move to establish a competitor to the World Bank.

> The so-called BRICS countries agreed to form an international development bank with aspirations to challenge the dominance of the World Bank and the International Monetary Fund.
>
> Leaders of Brazil, Russia, India, China and South Africa said Tuesday that the New Development Bank will start with $50 billion in capital and $100 billion as a currency reserve fund for liquidity crises. Operating details still need to be resolved.
>
> Still, the BRICS bank, which could add more member nations, represents a bid to expand the influence of the BRICS

> emerging markets and act as a counterbalance to institutions run by the U.S. and other developed nations, experts said.
>
> "This is about the consolidation of BRICS 2.0," said Marcos Troyjo, professor of international and public affairs at Columbia University and co-director of the BRICLab Center. "If BRICS 1.0 was about capturing investor attention to the scale of their economic relevance, BRICS 2.0 is about embarking on institution building."

I absolutely understand the reason for the move. These large countries have been demanding more influence over the World Bank for years, to no avail. And US policies like Quantitative Easing have been really damaging to some of the countries, particularly Brazil. Though, this move may well come too late for Brazil and certainly for Dilma Roussef.

> "I don't think that if Brazil was now to be thinking about these plans from the drawing board, it would really be thinking about a Brics development bank," says James Lockhart-Smith, a Latin America risk analyst at Maplecroft in New York. "It would be more focused on restarting growth in the country."
>
> But at a time of slow growth, Brazil probably needs these economies on side more than ever. Add to that, trade with economically troubled Argentina – traditionally one of its biggest trading partners – has become more difficult in recent years.

So while I understand the move, I wonder why now – aside from the fact that the World Cup provided a handy excuse for a meeting in Rio de Janeiro. It may be too late for Dilma, and India's new neoliberal Prime Minister Narenda

Modi seems like an odd fit for the group.

Meanwhile, consider this. While Russia won't get any of the big perks in the new bank (it will be headquartered in Shanghai, India will pick the first President, Brazil will pick the first Chairman, and the bank will be denominated in — really! — dollars), Putin was also making other interesting moves in the hemisphere, at least according to RT (definitely click through for Putin's expression, which surely is staged to be that stern).

> Moscow and Havana have reportedly reached an agreement on reopening the SIGINT facility in Lourdes, Cuba – once Russia's largest foreign base of this kind – which was shut down in 2001 due to financial problems and under US pressure.
>
> [snip]
>
> Russia considered reopening the Lourdes base since 2004 and has sealed a deal with Cuba last week during the visit of the Russian President Vladimir Putin to the island nation, reports Kommersant business daily citing multiple sources.

Russia shut down the base to more easily reschedule debt held by the US. Along with reopening the base, Russia will forgive a bunch of outstanding Cuban debt to Russia.

The timing of this — a year after Snowden's disclosures, but more importantly, as the US continues to try increasingly unilateral sanctions against Russia's involvement in Ukraine — makes a ton of sense. The US refuses to believe it can't impose its will in Ukraine, in spite of increasing reluctance from our European partners, especially Germany, to ratchet up the pressure. Reopening a front in America's back yard as the US bunkers down on Ukraine makes perfect sense.

For some reason, the US appears to have believed

it could simply impose its will indefinitely on the rest of the world. They appear not to have considered that, at some point, such behavior would provide the rest of the world cause to fight back.

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.

PAKISTAN'S GEO NOW ACCUSED OF BLASPHEMY: THAT COULDN'T HAPPEN HERE, COULD IT?

Just under a month ago, Pakistan's largest private television news station was engaged in a dispute with Pakistan's intelligence agency, ISI, over charges that the ISI was behind an assassination attempt on one of its anchors. For Geo, those probably seem like the good old days, because now the station is engaged in a controversy that has already caused a proliferation of lawsuits and threatens to erupt into massive vigilante violence against Geo employees and buildings. Reuters describes the threats Geo now faces and how the situation came about:

> Pakistan's biggest television station said it was ramping up security on

> Tuesday after it became the object of dozens of blasphemy accusations for playing a song during an interview with an actress.
>
> Geo Television is scrubbing logos off its vans and limiting staff movements after receiving scores of threats over allegedly blasphemous content, said channel president Imran Aslam.
>
> “This is a well-orchestrated campaign,” he told Reuters. “This could lead to mob violence.”
>
> /snip/
>
> The cases allege a traditional song was sung about the marriage of Prophet Muhammad’s daughter at the same time a pair of shoes was raised.
>
> Both elements are traditional in a wedding ceremony but the timing was insulting to Islam, dozens of petitioners have alleged. Others allege the song itself was insulting.

Lawsuits arising from the incident are proliferating. The Express Tribune has a partial list of the cases filed recently here.

But the Reuters article points out that under Pakistani law, blasphemy itself is not actually defined clearly:

> Blasphemy carries the death penalty in Pakistan but is not defined by law; anyone who says their religious feelings have been hurt for any reason can file a case.

But it gets even wilder. It turns out that a rival station is now also accused of blasphemy. Why? Because they repeatedly played snippets of the original program carried on Geo. And Reuters points out that blasphemy cases also are dangerous for judges and attorneys, as well:

> Advocate Tariq Asad said his suit named the singers and writers of the song, cable operators, television regulators, a national council of clerics and ARY, a rival television station.
>
> ARY repeatedly broadcast clips of the morning show, alleging it was blasphemous, an action that Asad said was blasphemous in itself.
>
> Judges frequently do not want to hear evidence in blasphemy cases because the repetition of evidence could be a crime. Judges acquitting those accused of blasphemy have been attacked; a defense lawyer representing a professor accused of blasphemy was killed this month.

So just repeating the blasphemous material, even as a judge or attorney citing it in court, is a blasphemous act in itself worthy of vigilante action.

But of course, nothing so outrageous could happen here in the US, could it? Sadly, such a ridiculous state of affairs doesn't seem that far off here. Note that politicians, even leading candidates for the US Senate, now openly state that "Government cannot force citizens to violate their religious beliefs under any circumstances" and even that such stances are not negotiable in any way. But that's not just a campaign stance. We have companies now going to the Supreme Court to state their right to ignore laws to which they object on religious grounds.

So if both politicians and companies now openly advocate to ignore laws on religious grounds, how far away are we from these same zealots advocating for prison terms or even death sentences for those who offend their religious sensibilities? After all, we have already seen a bit of the vigilantism that goes along with such attitudes.

Update: It turns out that the incident with ISI hadn't blown over yet. Breaking news from Dawn:

> A committee formed by the Pakistan Electronic Media Regulatory Authority (Pemra) has suspended the licences of three television channels owned by the Geo TV network.
>
> The committee has also decided that Geo TV offices be immediately sealed.
>
> However, a final decision on the revocation of the licences will be announced following the meeting on May 28, which will also be attended by government representatives.
>
> The committee, which includes members Syed Ismail Shah, Pervez Rathore and Israr Abbasi, was tasked to review the Ministry of Defence's application filed against Geo TV network for leveling allegations against an intelligence agency of Pakistan.

It will be interesting to see how Geo responds.

JEISH AL-ADL EXECUTES ONE OF FIVE IRANIAN BORDER GUARDS ABDUCTED LAST MONTH

There is a major new development in the ongoing saga of incidents along the Iran-Pakistan border. Recall that a group of Sunni extremists, Jeish Al-Adl, captured five Iranian border guards in early February (after killing 14 in an attack last October). Iran had briefly claimed that the guards had been released earlier this month, but then quickly backed down on that claim. It seems that Iran has difficulty getting accurate information on the status of the

guards, as they first denied and then finally confirmed that the highest ranking of the guards, Jamshid Danaeifar (his face is circled on a photo of the detained guards that is circulating on Twitter) has been executed:

> Informed sources in Pakistan confirmed earlier reports that Jeish al-Adl terrorist group has executed one of the five Iranian border guards that it abducted along Iran-Pakistan border on February 6.
>
> The sources told FNA in Islamabad on Monday that “Jeish al-Adl has martyred one of the kidnapped border guards”.
>
> This is while the Iranian Interior Ministry earlier today rejected Jeish al-Adl’s claim.
>
> “We don’t confirm this report; were it true, we would have been informed,” Interior Ministry Spokesman Hossein Ali Amiri said on Monday.He said that the five border guards are kept in Pakistan at present and are safe and sound.
>
> Amiri made the remarks after Jeish al-Adl claimed on its tweeter page that it has killed Jamshid Danayeefar, one of the kidnapped border guards.

News of the execution came just as Iran had been expressing hope that the guards were about to be released. From an earlier report on Sunday by Fars News:

> Efforts and consultations with the Pakistani officials still continue to secure the release of the five border guards abducted along Iran-Pakistan border on February 6, an Iranian official announced on Sunday.
>
> “Talks with national and local Pakistani officials have been held at different levels and they have made some promises,” Governor-General of Iran’s

> Southeastern Sistan and Balouchestan province Ali Awsat Hashemi told FNA today.
>
> He expressed the hope that the five young border guards would be released to return to their families soon.

Writing at the International Policy Digest, Sadaf Megan informs us that Jeish Al-Adl has stated that if their demands on the release of prisoners are not met, they will execute another prisoner in ten days:

> In the statement following the announcement of his death, Jaish al-Adl demands that if 50 of their prisoners are not released by Iran then Jaish al-Adl will execute another hostage within 10 days.
>
> The clock is ticking for the four remaining “pasdar(s)” or guards. In the meantime it seems unlikely that the Iranian government will be able to fulfill or want to meet the demands of Jaish Al-Adl. A regime that does not succumb to threats and ultimatums by the West is unlikely to make a deal with a terrorist group.

The article also has interesting background information on Jeish Al-Adl, providing perspective on the relationship with Jundallah:

> Jaish al-Adl operates in the Sistan-Baluchistan region of Iran, and frequently utilizes the Iranian-Pakistani border to carry out attacks. Cross border operations have been practiced during the time of Abdolmalek Rigi’s Sunni Balochi group, Jundallah. After Iran executed Rigi in 2010, Jundallah dissolved and merged with Jaish al-Adl.

Stay tuned for further developments. With Pakistan still reeling from the Carlotta Gall article the Express Tribune wound up censoring entirely because of its revelations of ISI sheltering bin Laden, they risk displaying more evidence of collaboration with terrorists if they are unable to secure the release of the remaining border guards before the next one is executed.

"IT'S TOUGH ON MY FAMILY:" A TALE OF TWO TEACHERS

"It's tough on my family," James Clapper said in an interview with the Daily Beast of observations he's a liar. Especially his son, who is a high school teacher (though Clapper didn't explain why his profession led his son to internalize accusations made against him).

> The charges against his integrity bother Clapper. "I would rather not hear that or see that," he said. "It's tough on my family, I will tell you that. My son is a high school teacher and he has a tendency, or he is getting over it, to internalize a lot of this."

And yet this man who thinks it unfair to question a public servant's integrity after he lies blatantly, who has no idea why Edward Snowden did what he did, why he leaked proof that the NSA was collecting the phone records of most Americans, why Snowden leaked evidence of bulk collection (that includes Americans) overseas, why he leaked details on the NSA's corruption of encryption.

Which made me think of a different teacher, Zaimah Abdur-Rahim, one of the plaintiff's in

the suit Judge William Martini dismissed last week.

Abdur-Rahim taught at the girls school surveilled by the NYPD – the school, which was accredited by the state of NJ – was actually in her home – and now teaches at another of the schools scoped out by the cops.

> Zaimah Abdur-Rahim resides at [address removed]. She is currently a math teacher at Al Hidaayah Academy ("AHA"), a position she has held since 2010. A record of the NYPD's surveillance of AHA appears in the Newark report, which includes a photograph and de scription of the school . Abdur-Rahim was also the principal of Al Muslimaat Academy ("AMA"), a school for girls grades five through twelve, from 2002 through 2010. Like AHA, a record of the NYPD's surveillance of AMA appears in the Newark report, including a photograph, the address, and notations stating, among other things, that the school was located in a private house and that the ethnic composition of the school was African American.
>
> Abdur-Rahim has been unfairly targeted and stigmatized by the NYPD's surveillance of AHA, where she is currently employed, and AMA, where she was last employed, as part of the Department's program targeting Muslim organizations. She reasonably fears that her future employment prospects are diminished by working at two schools under surveillance by law enforcement. Moreover, the Newark report's photograph of AMA is also Abdur-Rahim's home, where she has lived since 1993 with her husband and, at various times, her children and grandchildren. The fact that a photograph of h er home appears on the internet in connection with the NYPD's surveillance p rogram that the

> City of New York has since publicly exclaimed is necessary for public safety, has decreased the value of the home and diminished the prospects for sale of the home.

I'm betting that having her home and places of work surveilled by the cops is tough on Abdur-Rahim's family, far tougher than it is for Clapper's son to internalize complaints by the citizens he serves about the demonstrable obfuscation by his father.

There is no evidence that the NSA programs defended by Clapper ever specifically targeted Abdur-Rahim, though in this era of information sharing it is conceivable that NYPD identified potential targets (especially mosques) using data obtained indirectly from NSA.

But the entire system Clapper defends — in which communication ties between individuals serve, by themselves, as cause for further investigation — foments a logic that questions the integrity of great many members of the Muslim community. They get swept up in a dragnet (or exposed to infiltrators selected in part by using the dragnet) that targets them not because of what they said publicly in front of television cameras, which is why Clapper's integrity is under question, but simply because they are 2 or 3 degrees away from someone subjected to a virtual stop-and-frisk.

Imagine how the sons and daughters of the real live teachers targeted by Clapper's dragnet must internalize the presumption of a lack of integrity or even worse? Imagine how much worse it must be when the suspicion comes not from actual actions taken, lies told, but from ties to a community?

Clapper's plea for his own reputation here is ill-placed. It actually convinces me we're relying on the wrong evidence for questioning his integrity.

Because his actions, particularly over the past

4 years, involved questioning the integrity of many people based on far, far less evidence than is now being wielded against him. But when he and his employees at the National Counterterrorism Center question someone's integrity, in secret, with little recourse for appeal, there may be consequences, like losing the ability to fly, or receiving extra scrutiny when they do try to fly.

And he still doesn't get the problem with that. He still doesn't understand why his "so-called" domestic surveillance —and the foreign surveillance that also sucks up Americans — is so much worse than being held to account for lies you tell Congress.

THE NSA MAY NOT "TARGET" LAWYERS, BUT IT DOES "SPY" ON THEM

Congratulations to Ben Wittes who, with this post, demonstrates how the NSA can "spy" on Americans without "targeting" them.

His piece consists of several steps. First, Wittes goes to great effort to show that Laura Poitras and James Risen have not shown that the American law firm representing the Indonesian government, Mayer Brown, was "targeted" (though he seems to think that means they weren't spied on).

> For starters, it is important to emphasize that the *Times* story does not involve NSA spying. It doesn't involve any remotely-plausible suggestion of illegality. It doesn't involve any **targeting** of Americans. And it doesn't involve any **targeting** of lawyers either.

> The facts the story reports are these:
>
> - *The surveillance in question was conducted by the Australian Signals Directorate (ASD), not NSA.*
> - *The surveillance targeted Indonesian government officials engaged in trade talks with the United States.*
> - *The surveillance apparently took place overseas. (There is no suggestion in the story that the surveillance took place inside the United States.)*
>
> In other words, a foreign intelligence service was conducting surveillance against another foreign government, which was in communication with a U.S. law firm. [my emphasis]

This is a flimsy use of NSA's own euphemism, "targeting," given that NYT never uses the word in the context of the law firm (they do use it to discuss the law and make it clear ASD discovered they were spying on an American who was working for the USG). The verbs they use include "entangled," "caught up," "monitored," "ensnared," and "compromised." All verbs that describe what happens when someone talks to a targeted entity.

From there, Wittes takes a hypothetical quote offered by the NSA spokesperson, explaining that NSA sometimes does ask Five Eyes partners to take special precautions, to suggest the NSA did ask Australia's ASD to protect the US lawyers

involved.

> An N.S.A. spokeswoman said the agency's Office of the General Counsel was consulted when issues of potential attorney-client privilege arose and could recommend steps to protect such information.
>
> "Such steps could include requesting that collection or reporting by a foreign partner be limited, that intelligence reports be written so as to limit the inclusion of privileged material and to exclude U.S. identities, and that dissemination of such reports be limited and subject to appropriate warnings or restrictions on their use," said Vanee M. Vines, the spokeswoman.

But doesn't quote the bit that makes it clear NSA would not — and was not — commenting on this case.

> The N.S.A. declined to answer questions about the reported surveillance, including whether information involving the American law firm was shared with United States trade officials or negotiators.

Then Wittes shows the ambiguity about what happened when the ASD told the US an American law firm had gotten caught in its surveillance, quoting from the text.

Here's the direct quote from the document in question.

> (TS//SI//REL) **SUSLOC Facilitates Sensitive DSD Reporting on Trade Talks**: According to SIGINT information obtained by DSD, the Indonesian Government has employed a US law firm to represent its interests in trade talks with the US. On DSD's behalf, SUSLOC sought NSA OGC guidance regarding continued reporting

> on the Indonesian government communications, taking into account that information covered by attorney-client privilege may be included. OGC provided clear guidance and DSD has been able to continue to cover the talks, providing highly useful intelligence for interested US customers.

Now, I agree this passage is not crystal clear (though it is less ambiguous than the text itself). What is clear is DSD (the name of which has subsequently been changed to ASD) continued spying on the Indonesian government — and sharing that spying with US "customers" — after SUSLOC consulted (on its behalf) with NSA's lawyers.

Wittes then points to how Section 702 minimization procedures (he admits the minimization under EO 12333 in this case would be weaker) would "protect" these conversations — and after almost 300 words, admits that even the more stringent Section 702 procedures offer no specific protections for attorneys in a civil matter.

> NSA cannot target anyone for Section 702 collection—not even foreign persons overseas—without a valid foreign intelligence purpose. Section 702 categorically forbids intentionally targeting any U.S. person—or any other person believed to be inside the U.S. And it requires NSA to follow procedures to minimize any information acquired in the course of targeting non-U.S. persons reasonably believed to be located outside the United States. So it would be legal to target Indonesian officials engaged in trade talks with the United States, but NSA would have to discard any communications they might have with US persons—lawyers or not—to the extent there was no foreign intelligence value in those communications. And NSA would have to discard and mask the US persons'

> identities except to the extent that those identities themselves had foreign intelligence value.
>
> According to section 4 of the declassified 2011 guidelines governing minimization, moreover, additional protections kick in when it becomes apparent that acquired communications are taking place between any person known to be under criminal indictment in the United States and an attorney representing that individual in the matter. Monitoring of that communication must halt, the communication must be segregated from other acquired information and special precautions must be taken through the DOJ's National Security Division to ensure the communications play no part in any criminal prosecution. As an added precaution, the NSA Office of General Counsel is also required to review all proposed disseminations of U.S. person attorney-client privileged communications prior to dissemination.
>
> The 2011 minimization guidelines aren't airtight; critics have pointed out that calls that fall under attorney-client privilege need not be minimized if the target has not been criminally charged under U.S. law. And **they thus would not protect attorney-client communications in a civil matter like a trade negotiation at all**.

Which is a long-winded way of saying that even if the NSA followed more stringent Section 702 minimization procedures, even if it were conducting the collection directly rather than through a Five Eyes agreement, even if it were collecting data in the US, it could continue to collect these conversations and disseminate the content of them so long as it didn't disseminate the identities of the US persons involved.

Of course, that the NYT was able, with very little evidence, to identify with a high degree of certainty the firm and lawyers involved shows what that's worth.

So upon consultation, the ASD would have been told that even US rules on domestic spying would not prevent the NSA from spying on Mayer Brown off targeting directed at the Indonesian government. And all that's all ignoring that US persons get less protection under EO 12333.

So however you want to fetishize the word "target," what seems clear from the story is that a Five Eyes partner shared information with US customers, almost certainly including what should be the content of privileged attorney-client communications, on a matter in which the US was the legal adversary. That NSA did not push the button does not alter the clear implication that the US was collecting, via its partner relationships, legally protected information on a party they were in a legal dispute with.

But this is not news!!!!

After all — in a case that has become central to the current legal understanding of FISA — the NSA not only spied on Wendell Belew's conversations when he was representing the Muslim charity al-Haramain (conversations he engaged in from the US), but they sent him a log of the conversations they spied on! There, like here, you could say the US didn't "target" the lawyer (they almost certainly targeted his client, Soliman al-Buthi), but the effect is still the same, listening in on privileged conversations in which the US is the adversary.

And if you think all that ended with the Bush administration, consider the case of Robert Gottlieb, all of whose pre-indictment calls with his client Adis Medunjanin (Najibullah Zazi's co-conspirator), were recorded.

> The first time Adis Medunjanin tried to call Robert C. Gottlieb in mid-2009, Gottlieb was out of the office.

> Medunjanin was agitated. He had to speak to an attorney. Gottlieb's assistant told him Gottlieb would be back soon. When Medunjanin spoke to the lawyer a little later, he was told he might need legal representation. He thought he might be under investigation.
>
> Over the next six months and in forty-two phone calls, Medunjanin sought legal advice from Gottlieb. When he was arrested in January 2010 on charges that he tried to bomb the New York subway, it was Gottlieb who defended him, receiving security clearance to review government documents pertinent to the case in the process.
>
> Gottlieb was preparing Medunjanin's defense when a federal officer in charge of information distribution e-mailed him that there was new classified information he needed to review at the US Eastern District Court in Brooklyn. "I went over to the Brooklyn Federal courthouse, went up to the secured room, gained entry with the secret security codes, opened the file cabinet that is also secure and in the second drawer was a CD," Gottlieb told me. On that CD were recordings of every single one of his forty-two phone calls with Medunjanin before he was taken into custody and indicted on January 7, 2010.

In this case, we know the government had a FISA warrant for Medunjanin (Enemies Within even tells us the FISA warrants were filed in NY). So we know that Gottlieb was not "targeted." But that didn't stop the government from collecting and listening to 42 privileged phone conversations between two American citizens taking place entirely within the US.

And all of these — the presumed case of Mayer Brown, the proven case of al-Haramain, and the proven case of Medunjanin — would have adhered

to the Section 702 minimization procedures NSA apologists point to as some great protection for legally privileged conversations (though the surveillance of all of them took place under different authorities).

That should not lead anyone to believe — much less claim — that this means the US government doesn't spy on lawyers. On the contrary, it should demonstrate that no matter how many times someone wields the words "target" and "minimization procedures," it still permits the NSA to spy on privileged conversations between lawyers and their clients, with the only marginally meaningful protections offered to indicted defendants. Indeed, it should demonstrate how the NSA's special carve out for attorney client conversations doesn't amount to anything for the great majority of legally privileged conversations.

The entire point of spying — whether directly or via a partner, whether in the US or overseas — is getting the substance of communications. And NSA's minimization procedures allows them to do that in the case of a great deal of attorney-client conversations. We should not be surprised they've used that permission on multiple occasions.

Update: "So upon consultation" sentenced added for clarity.

PCLOB REPORT, WORKING THREAD

The report is here. I will do a running update of my comments. Page references will be to the report page numbers, not PDF.

(4) Note PCLOB had access to "various inspector general reports."

(6) Note the dates when WH got these conclusions.

(9) PCLOB confirms what I was the first to point out: this program operated without a legal opinion until July 2013. Told ya so.

(10) One of four reasons the program is illegal is bc 215 is written for FBI, not NSA. Also says it violates ECPA.

(11) PCLOB says FBI would have found Moalin w/o the dragnet. Remember, they were investigating his hawala and had a tap on Ayro.

(14) PCLOB confirms only two cases (info sharing/minimization and Yahoo) ever got to FISCR.

(15) On the govt's so-called transparency:

> However, to date the official disclosures relate almost exclusively to specific programs that had already been the subject of leaks, and we must be careful in citing these disclosures as object lessons for what additional transparency might be appropriate in the future.

(17) PCLOB provides several immediate relationships and notes that Obama doesn't need Congress to do them.

(19) Note PCLOB's reference to releasing opinions on programs that have been discontinued bc of continuing relevance. Suspect this refers to more than just the Internet dragnet.

(25) Note PCLOB says the data integrity analysts take out "other unwanted data" in addition to high volume numbers. I believe some sensitive numbers are purged at this step.

(30) PCLOB dances around saying that corporate store leads right to content.

> For instance, such calling records may be integrated with data acquired under other authorities for further analysis

(31) PCLOB notes FBI gets reports on the dragnet. It doesn't mention CIA and NCTC or other agencies.

(32) CIA and NCTC have no minimization rules for data that comes from 215 reports:

> Other federal agencies also receive information from the NSA that was obtained through Section 215, but the FISA court's orders do not establish rules for how those agencies must handle the information they receive.83 In addition, the government has informed the FISA court that it may provide telephone numbers derived from the program to "appropriate . . . foreign government agencies."84

(33) PCLOB notes that FISC doesn't say what kind of training the dragnet people must get. As a former training professional, their training sucks ass.

(34) Nice description of the monthly reports.

(40) The phrasing for the description of what happened with the Internet dragnet is very interesting.

> After several years of operation, which included significant incidents of noncompliance with the FISA court's orders, the bulk collection of Internet metadata under FISA court approval was terminated. Upon concluding that the program's value was limited, the NSA did not seek to renew it.

(40) PCLOB points to the USA Today reporting on the phone dragnet program to explain the telecom urgency for a legal order. That was May 10, the first dragnet order was May 24. They did it in two weeks.

(41) PCLOB makes it clear the government was already planning on moving to Section 215 when the extension was passed in 2006.

> The collection of telephone records under the President's Surveillance Program was classified, however, and the government's plans to seek new legal authority for that collection were not made public. Thus, congressional debates about the terms on which Section 215 should be renewed included no public discussion of the fact that the executive branch was planning to place the NSA's bulk calling records program under the auspices of the reauthorized statute.

(43) Note reference to John Scott Redd.

(44) PCLOB distinguishes the phone dragnet from the Internet one bc the latter was only taking circuits commonly used by terrorist traffic.

(45) The reference to minimization procedures and 2702 in succession makes it clear that Walton's December 2008 response on 2702 was a response to Glenn Fine's IG Report.

(46) Note the [sic] on numbers in the footnote.

(47) PCLOB, like I did, points out the 2009 problems came from continuing features of the illegal program.

(54) Here's a list of the other violations in the phone dragnet. I suspect they're described in the orders the Admin is still withholding.

> The isolated incidents reported to the FISA court comprised the following violations: (1) The NSA inadvertently received a tiny amount of cell site location information from a provider on one occasion (the data was accessible only to technical personnel and was never available to intelligence analysts); (2) An analyst performed a query on a selection term whose RAS approval had expired earlier that month (the agency responded with technical modifications to prevent such

> incidents); (3) A RAS determination was made based on what was later discovered to be incorrect information (the resulting query results were destroyed, and no intelligence reports were issued based on the query); (4) On several occasions analysts shared the results of queries via email with NSA personnel who were not authorized to receive such information (the agency responded with new procedures for email distribution); (5) An analyst sent an email message containing information derived from the Section 215 data to the wrong person, due to a typographical error in the email address (the recipient reportedly deleted the message without reading it, recognizing the error); (6) Information about U.S. persons was on three occasions disseminated outside the NSA before any official made the determinations that are required for such disseminations (officials later concluded that the standards for dissemination were satisfied in each case); (7) The government filed nine reports with the FISA court that lacked certain information required to be in such reports (the missing information involved no wrongdoing or noncompliance, and it subsequently was furnished to the court); (8) The government filed a compliance report with the FISA court on a Monday, instead of on the deadline the previous Friday.
>
> The two other noncompliance incidents were more far-reaching, although both represented inadvertent violations. In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the applicable retention rules. These files were among those used in connection with

> a migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit. The technical server in question was not available to intelligence analysts.
>
> In the other incident, the NSA discovered that it had unintentionally received a large quantity of customer credit card numbers from a provider. These related to cases in which a customer used a credit card to pay for a phone call. This problem, which involved cases in which customers used credit cards to pay for phone calls, resulted from a software change implemented by the provider without notice to the NSA. In response to the discovery, the NSA masked the credit card data so that it would not be viewable for intelligence analysis. It also asked providers to give advance notice of changes that might affect the data transmitted to the NSA. The agency later eliminated the credit card data from its analytic stores, although the data remained in the agency's non-analytic online stores and in back-up tapes. Despite repeated efforts to attempt a technical fix, six months later the agency was still receiving a significant amount of credit card information from the provider. As a result of additional efforts, this was reduced to fewer than five credit card numbers per month, and the provider continued to work to eliminate such production entirely.

(58) My favorite line so far:

> Notably, Section 215 requires that records sought be relevant to 'an' authorized investigation.

(61) The PCLOB smackdown on the legal logic behind the dragnet is delightful (is anyone here familiar enough w/Wald's judicial style to tell me whether this is all her?). The passage on "necessity" is important because it pushes back on underlying claims in OLC memos.

(65) We keep talking about the scope of the data NSA gets. This suggests it's closer to "all."

> As to that type of record, however, the government seeks access to virtually everything.

(69) Ow. I always suspected the White Paper citations on civil discovery were manufactured. PCLOB rips it to shreds.

(73) FN 267 argues Govt has a burden to show relevance. Somewhere, FISC even argued they were presumed regular.

(74) Note reference to House Report on PATRIOT debate—govt was looking for administrative subpoenas.

(80) Reading PCLOB's discussion of the need to have a belief makes me realize that belief was used as the same kind of dodge in the 215 argument as it was in the torture context.

(82) PCLOB calls the phone dragnet "an ongoing surveillance tool." Someone alert DiFi.

(94) PCLOB notes that NSL standards for phone metadata are actually higher than 215 standards. Given my suspicion FBI uses bulk NSLs for subscribe info, I find that partiularly interesting.

(96) I believe I've made this point too: given that there was no judicial opinion that approved the dragnet before it was reauthorized, Congress cannot be said to have authorized it.

(96) I like this:

> Applying the reenactment doctrine to legitimize the government's interpretation of Section 215, therefore, is both unsupported by legal precedent and unacceptable as a matter of democratic accountability.

(97) PCLOB is unaware that the Executive had not complied w/FAA requirements to share legal opinions on at least some of the Section 215 materials. (98) Hahaha! PCLOB did, at least, note that HPSCI did not pass on the 2011 notice to Congress. (99) PCLOB again suggests that the dragnet is designed to collect all call data.

> While the briefing paper explains that the NSA's program operates "on a very large scale" and involves "substantially all" of the calling records generated by "certain" telephone companies, it does not make explicit that the program is designed to collect the records of essentially all telephone calls.

(103) A novel idea:

> And we recommend as a policy matter that all three branches of government, in developing and assessing data collection programs, look beyond the application of cases decided in a very different environment and instead consider how to preserve the underlying constitutional principles in the face of modern communications technology and surveillance capabilities.

(133) PCLOB suggests the only thing protecting the dranget (in, for example, Amnesty v Clapper) from a First Amendment review is standing.

> However, in the cases decided so far, the Court has not reached the underlying question of whether the First Amendment

> has been violated, because the Court has found that the individuals challenging the surveillance program are not legally entitled to do so because they are unable to show that they are directly affected by the monitoring.

(140) PCLOB associates the Exigent Letters IG Report to this program. Says AT&T provided 2 hops on community of interest. Note the observation that AT&T could do 2 hops is new and not in unredacted text.

(144) PCLOB makes clear what I've been saying: the phone dragnet leads to the content.

> Any attempt to assess the value of the NSA's telephone records program must be cognizant of a few considerations. First, the information that the NSA obtains through Section 215 is not utilized in a vacuum. Rather, it is combined with information obtained under different legal authorities, including the Signals Intelligence that the NSA captures under Executive Order 12333, traditional wiretaps and other electronic surveillance of suspects conducted under FISA court authority, the interception of telephone calls and emails authorized by the FISA Amendments Act of 2008, the collection of communications metadata through FISA's pen register and trap and trace provision, physical surveillance, and the development of informants. The intelligence community views the NSA's Section 215 program as complementing and working in tandem with these and other intelligence sources, enabling analysts to paint a more comprehensive a picture when examining potential national security threats.

(155) PCLOB raises a point I have: why didn't the dragnet find the other unsuccessful attacks?

> Yet, it is worth noting that the program supplied no advance notice of attempted attacks on the New York City subway, the failed Christmas Day airliner bombing, or the failed Times Square car bombing.

(182) Note PCLOB met with John Bates. Interesting that neither PCLOB nor the Review Group were very sympathetic to FISC concerns.

(193) Mike Rogers has been warned.

> We expect to return to transparency in our future work.

(205) On 12333

> Our suggestions here focus on FISA authorities and are also relevant to National Security Letters. Our recommendations do not address reporting of activities under Executiv e Order 12333. It has become clear in recent months that E.O. 12333 collection poses important new questions in the age of globalized communications networks, but the Board has not yet attempted to address those issues.

(210) One of Brand's excuses for why PCLOB shouldn't weigh in on law?

> This legal question will be resolved by the courts, not by this Board, **which does not have the benefit of traditional adversarial legal briefing** and is not particularly well – suited to conducting de novo review of long – standing statutory interpretations