“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 CORPORATE STORE: WHERE NSA GOES TO SHOP YOUR CONTENT AND YOUR LIFESTYLE

I'm increasingly convinced that for seven months, we've been distracted by a shiny object, the phone dragnet, the database recording all or almost all of the phone-based relationships in the US over the last five years. We were never wrong to discuss the dangers of the dragnet. It is the equivalent of a nuclear bomb, just waiting to go off. But I'm quite certain the NatSec establishment decided in the days after Edward Snowden's leaks to intensify focus on the actual construction of the dragnet — the collection of phone records and the limits on access to the initial database (what they call the collection store) of them — to distract us away from the true family jewels.

A shiny object.

All that time, I increasingly believe, we should have been talking about the corporate store, the database where queries from the collection store are kept for an undisclosed (and possibly indefinite) period of time. Once records get put in that database, I've noted repeatedly, they are subject to "the full range of [NSA's] analytic tradecraft."

We don't know precisely when that tradecraft gets applied or to how many of the phone identifiers collected in any given query. But we know that tradecraft includes matching individuals' various communication identifiers (which can include phone number,

handset identifier, email address, IP address, cookies from various websites) — a process the NSA suggests may not be all that accurate, but whatever! Once NSA links all those identities, NSA can pull together both network maps and additional lifestyle information.

> The agency was authorized to conduct "large-scale graph analysis on very large sets of communications metadata without having to check foreignness" of every e-mail address, phone number or other identifier, the document said.
>
> [snip]
>
> The agency can augment the communications data with material from public, commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information, as well as property records and unspecified tax data, according to the documents. They do not indicate any restrictions on the use of such "enrichment" data, and several former senior Obama administration officials said the agency drew on it for both Americans and foreigners.

That analysis might even include tracking a person's online sex habits, if the government deems you a "radicalizer" for opposing unchecked US power, even if you're a US person.

Such profiles are not the only thing included in NSA's "full range of analytic tradecraft."

We also know — because James Clapper told us this very early on in this process — the metadata helps the NSA pick and locate which content to read. The head of NSA's Signals Intelligence Division, Theresa Shea, said this more plainly in court filings last year.

> Section 215 bulk telephony metadata

> complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, **while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities**. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

The NSA prioritizes reading the content that involves US persons. And the NSA finds it, and decides what to read, using the queries that get dumped into the corporate store (presumably, they do some analytical tradecraft to narrow down which particular conversations involving US persons they want to read).

And there are several different kinds of content this might involve: content (phone or Internet) of a specific targeted individual — perhaps the identifier NSA conducted the RAS query with in the first place — already sitting on some NSA server, Internet and in some cases phone content the NSA can go get from providers after having decided it might be interesting, or content the NSA collects in bulk from upstream collections that was never targeted at a particular user.

The NSA is not only permitted to access all of this to see what Americans are saying, but in all but the domestically collected upstream

content, it can go access the content **by searching on the US person identifier**, not the foreign interlocutor, without establishing even Reasonable Articulable Suspicion that it pertains to terrorism (though the analyst does have to claim it serves foreign intelligence purpose). That's important because lots of this content-collection is not tied to a specific terrorist suspect (it can be tied to a geographical area, for example), so the NSA can hypothetically get to US person content without ever having reason to believe it has any tie to terrorism.

In other words, all the things NSA's defenders have been insisting the dragnet **doesn't** do — it doesn't provide content, it doesn't allow unaudited searches, NSA doesn't know identities, NSA doesn't data mine it, NSA doesn't develop dossiers on it, even James Clapper's claim that NSA doesn't voyeuristically troll through people's porn habits — every single one **is** potentially true for the results of queries run three hops off an identifier with just Reasonable Articulable Suspicion of some tie to terrorism (or Iran). Everything the defenders say the phone dragnet is not, the corporate store is.

All the phone contacts of all the phone contacts of all the phone contacts of someone subjected to the equivalent of a digital stop-and-frisk are potentially subject to all the things NSA's defenders assure us the dragnet is not subject to.

Don't get me wrong: I'm not saying some of this analysis isn't appropriate with actual terrorist suspects.

But that's not what the corporate store is. It is — PCLOB estimates — up to 120 million phone users (the actual number of people would be smaller because of burner phones, and a significant number would be foreign numbers), the overwhelming majority of which are completely innocent of anything but being up to 3 degrees away from a guy who got digitally

stop-and-frisked.

Yet those potentially millions of Americans get no effective protection once they're in the corporate store. As the PCLOB elaborates,

> Once contained in the corporate store, analysts may further examine these records without the need for any new reasonable articulable suspicion determination.
>
> [snip]
>
> Furthermore, under the rules approved by the FISA court, NSA personnel may then search any phone number, including the phone number of a U.S. person, against the corporate store — as long as the agency has a valid foreign intelligence purpose in doing so — without regard to whether there is "reasonable articulable suspicion" about that number. 589 Unlike with respect to the initial RAS query, the FISA court's orders specifically exempt the NSA from maintaining an audit trail when analysts access records in the corporate store. 590

There are just a few protections. The analysts accessing the corporate store need to have undergone training and must claim a foreign intelligence (but not exclusively counterterrorism) purpose. And normally, if NSA wants to circulate the US person data outside of the NSA, a high level official must certify that,

> the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.

Again, that doesn't require the US person have any tie to counterterrorism, just that it be

"related to" counterterrorism, which FISC has already deemed even the larger collection store to be by default. (The Executive Branch can also search the corporate store for exculpatory or inculpatory information, which, given that no defendant has succeeded in getting a search for the former, probably means it is only used for the latter — and note, this is **not**, apparently, limited to counterterrorism purposes, and as of right now the Executive is also permitted to do back door searches of content for criminal evidence unrelated to terrorism, though Obama has vaguely promised to change that while stopping short of a warrant.)

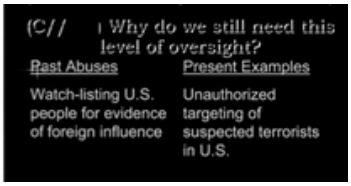
And no one, aside from PCLOB's estimate of up to 120 million (which may or may not have been reviewed when PCLOB let the IC review some of their process descriptions), is talking about how many Americans are in the corporate store. Geoffrey Stone has said NSA only "touched" 6,000 people in 2012, though that may mean only 6,000 of a much larger number of people who got placed in the corporate store were subjected to further NSA processing. We can assume the numbers were far higher until 2009, when there were over 17,000 on a RAS list. Furthermore, I'm very curious to see whether such numbers spike for 2013, given claims that NSA used the dragnet for "peace of mind" after the Boston Marathon attack, launched by young men who interacted via mobile phone with a huge number of totally innocent US person contacts. Will half of Cambridge, MA be subject to the full range of NSA's tradecraft because we used the dragnet to get peace of mind after the Boston Marathon attack?

Moreover, as discussed last month, the NSA can alter the intake into the corporate store via choices made by data integrity analysts — the other part of the process largely exempted from oversight, and with a few inclusions could cause the bulk of American call records to end up in the corporate store.

Obama said the dragnet "does not involve the NSA

examining the phone records of ordinary Americans." But in doing so, he was implying that the millions of Americans whose records may have made it into the corporate store are not ordinary, and therefore not entitled to the kind of due process enshrined in the Constitution.

PROJECT MINARET 2.0: NOW, WITH 58% MORE ILLEGAL TARGETING!



For weeks, I have been trying to figure out why the NSA, in a training program it created in August 2009, likened one of its "present abuses" to Project Minaret. What "unauthorized targeting of suspected terrorists in the US" had they been doing, I wondered, that was like "watch-listing U.S. people for evidence of foreign influence."

Until, in a fit of only marginally related geekdom, I re-read the following passage in Keith Alexander's declaration accompanying the End-to-End review submitted to the FISA Court on August 19, 2009 (that is, around the same time as the training program).

> Between 24 May 2006 and 2 February 2009, NSA Homeland Mission Coordinators (HMCs) or their predecessors concluded that approximately 3,000 domestic telephone identifiers reported to Intelligence Community agencies satisfied the RAS standard and could be used as seed identifiers. However, at the time these domestic telephone identifiers were designated as RAS-approved, **NSA's OGC**

> **had not reviewed and approved their use as "seeds" as required by the Court's Orders**. NSA remedied this compliance incident by re-designating all such telephone identifiers as non RAS-approved for use as seed identifiers in early February 2009. NSA verified that although some of the 3,000 domestic identifiers generated alerts as a result of the Telephony Activity Detection Process discussed above, none of those alerts resulted in reports to Intelligence Community agencies. 7
>
> 7 The alerts generated by the Telephony Activity Detection Process did not then and does not now, feed the NSA counterterrorism target knowledge database described in Part I.A.3 below. [my emphasis]

As I'll explain below, this passage means 3,000 US persons were watch-listed without the NSA confirming that they hadn't been watch-listed because of their speech, religion, or political activity.

Here's the explanation.

The passage actually appears in an entirely different part (PDF 37, document 81) of Alexander's declaration from his discussion of the alert list violations (PDF 30, document 74) that started the review of the phone dragnet program. But given the February (2009) timing and the discussion of Telephony Activity Detection alerts, this passage clearly addresses alerts violations.

Before I parse the passage, a few reminders about the NSA's multiple metadata dragnets and the alert system.

The NSA has an interlocking system of metadata query interfaces which we now know mix EO 12333 collected data with data collected under the US based phone and Internet dragnet programs. Data collected overseas is dumped in with data

collected directly from Verizon.

The interlocking system apparently does a lot of nifty things, one of which is to alert NSA if any of a watch-list of numbers have had certain kinds of phone activity in the previous day (the NSA has not explained what it does when it receives such alerts, which is part of the issue here). There were over 17,000 people on that list when the NSA first started cleaning up its phone dragnet problem.

The problem with having all that data mixed up in one system is that the standards for access are different based on where the data came from. For EO 12333 collected data (the data collected overseas) there's a foreign intelligence assumption that requires only a valid foreign intelligence purpose; this data can be accessed fairly broadly.

Whereas both the phone (BR) and Internet (PR/TT) dragnets — in which the data was collected by legal process in the United States — require "Homeland [ack!] Mission Coordinators" within the NSA to sign off on a claim that there is Reasonable Articulable Suspicion that the identifier belongs to someone with a tie to certain approved terror (and Iran) groups — it's basically a digital stop-and-frisk standard signed off by a manager.

That difference between EO 12333 and domestic dragnets created the first problem with the alert list: 90% of the people on the alert list had not had that bureaucratic sign-off, and so should not have been used with the BR phone dragnet data at all. That's the part of the alert problem we hear most about.

But in addition to the "RAS approval" step for the BR phone dragnet, there's an additional bureaucratic step for US persons.

The statute only permits Section 215 to be used against Americans,

> provided that such investigation of a United States person is not conducted

> solely upon the basis of activities protected by the first amendment to the Constitution.

The FISC orders (here's the one in place when NSA first started admitting the problem) accomplished that by reiterating that restriction (7-8) and mandating that,

> NSA's OGC shall review and must approve proposed queries of archived metadata based on "seed" telephone identifiers reasonably believed to be used by U.S. persons before any query is conducted. (8-9)

Note the "archived metadata" language. The NSA maintained that since the alert process happened as the data came into the database, that didn't count as a query of archived metadata. Judge Walton was not impressed.

The NSA had to get its lawyers to sign off on an assertion that the US person identifiers they were using to query the database had not been selected based solely on their religion, their speech, or political activity.

In other words, before NSA could use that US person's identifier either to query the dragnet (which produces a three-degrees of Osama bin Laden report) or to generate alerts, they should have had it RAS-approved by a Homeland [sic] Mission Coordinator **and** undergo a First Amendment review at OGC.

When I was first learning how to write effective bureaucratic documents 20 years ago, I learned that "shall" is the only magic word that can make people do what they're supposed to do; it's the only thing that conveys legal obligation. Apparently it didn't work out that way in this case, because 3,000 US persons — **58% more people than were on the Project Minaret watchlist**, which extended over 3 more years — were on (at a minimum) the alert list without that First Amendment review.

3,000 US persons (that is, either permanent residents or American citizens) were having their communications tracked because of a stop-and-frisk standard suspected tie to terrorism, without NSA affirming that they weren't being tracked because they were politically active Muslims or similar protected behavior.

Retrospectively, it's now clear that this exposure of Americans without First Amendment review was chief among Reggie Walton's concerns when he first responded to the dragnet. It's equally clear that Walton was just learning about the EO 12333 data on the alert list, including that US persons might be included on it.

> The preliminary notice from DOJ states that the alert list includes telephone identifiers that have been tasked for collection in accordance with NSA's SIGINT authority. What standard is applied for tasking telephone identifiers under NSA's SIGINT authority? Does NSA, pursuant to its SIGINT authority, task telephone identifiers associated with United States persons? If so, does NSA limit such identifiers to those that were not selected solely upon the basis of First Amendment protected activities?

~~DOJ and Keith Alexander were in no rush to answer Walton's question — the only unredacted response to his question about what happened with US persons~~ The NSA explained,

> Additionally, NSA determined that in all instances where a U.S. identifier served as the initial seed identifier for a report (22 of the 275 reports), the initial U.S. seed identifier was either already the subject of FISC-approved surveillance under the FISA or had been reviewed by NSA's OGC to ensure that the RAS determination was not based solely on a U.S. person's first amendment-

> protected activities.

That response was dated February 12, 2009, so Walton's response may have been to point out that alerts were effectively queries and a bunch of Americans were being tracked illegally. Note, too, that they're only telling Walton about queries that resulted in report to the FBI or some other agency; they're not denying that these identifiers were used for queries, which would have resulted in the numbers of their contacts being dumped into the corporate store forever.

But there are a few more details from Alexander's declaration, above, that should cause us concern:

- Rather than review these selectors to see if they had been selected based on their speech, religion, or politics, NSA's OGC simply moved them into a category — non-RAS approved — where such restrictions no longer applied. I would suggest their unwillingness to do such a review is rather striking.
- "Some of the 3,000 domestic identifiers generated alerts as a result of the Telephony Activity Detection Process." They shouldn't have been matched up against the incoming phone dragnet data, but it appears they were, and did produce those kinds of alerts, though NSA rather

conspicuously declines to tell us how many people that happened to and how often. We don't know what happened to these 3,000 US person or the people they communicated with after NSA discovered these daily contacts.

- The footnote notes that being on the alert list does not automatically put one in the "counterterrorism target knowledge database," NSA's tracker for suspected terrorists. But the footnote doesn't say that they weren't put in that database, potentially in part because of the alerts. Moreover, these "approximately 3,000 domestic telephone identifiers" had already gotten "reported to Intelligence Community agencies." While NSA makes much out of the fact that no query reports got sent on to the FBI and other agencies, that's sort of moot, because the identifiers, if not the names, already had been.

Mind you, to get disseminated to other agencies, these US person identities (if they were treated as such) would need to get sign-off for their intelligence value. Which is why I find OGC's solution — to avoid doing a First Amendment

review on them at all — so suspicious. Because high ranking NSA personnel had already done a review, and for some reason were unwilling to do further scrutiny.

3,000 US persons were on a watchlist, potentially because of their religion, politics, or speech. The NSA itself appears to have seen the similarities with Project Minaret, decades earlier.

But we keep hearing there were no abuses.

Updated erroneous link to Keith Alexander declaration.

Update, March 11: The NSA actually did provide more response on EO 12333 collection to Walton, which I hope to return to.

FISA WARRANTED TARGETS AND THE PHONE DRAGNET

The identifiers (such as phone numbers) of people or facilities for which a FISA judge has approved a warrant can be used as identifiers in the phone dragnet without further review by NSA.

From a legal standpoint, this makes a lot of sense. The standard to be a phone dragnet identifier is just Reasonable Articulable Suspicion of some tie to terrorism — basically a digital stop-and-frisk. The standard for a warrant is probable cause that the target is an agent of a foreign government — and in the terrorism context, that US persons are preparing for terrorism. So of course RAS already exists for FISC targets.

So starting with the second order and continuing since, FISC's primary orders include language approving the use of such targets as identifiers

(see ¶E starting on page 8-9).

But there are several interesting details that come out of that.

Finding the Americans talking with people tapped under traditional FISA

First, consider what it says about FISC taps. The NSA is already getting all the content from that targeted phone number (along with any metadata that comes with that collection). But NSA may, in addition, find cause to run dragnet queries on the same number.

In its End-to-End report submission to Reggie Walton to justify the phone dragnet, NSA claimed it needed to do so to identify all parties in a conversation.

> Collections pursuant to Title I of FISA, for example, do not provide NSA with information sufficient to perform multi-tiered contact chaining [redacted]Id. at 8. NSA's signals intelligence (SIGINT) collection, because it focuses strictly on the foreign end of communications, provides only limited information to identify possible terrorist connections emanating from within the United States. Id. For telephone calls, signaling information includes the number being called (which is necessary to complete the call) and often does not include the number from which the call is made. Id. at 8-9. Calls originating inside the United States and collected overseas, therefore, often do not identify the caller's telephone number. Id. Without this information, NSA analysts cannot identify U.S. telephone numbers or, more generally, even determine that calls originated inside the United States.

This is the same historically suspect Khalid al-Midhar claim, one they repeat later in the passage.

The language at the end of that passage emphasizing the importance of determining which calls come from the US alludes to the indexing function NSA Signals Intelligence Division Director Theresa Shea discussed before — a quick way for the NSA to decide which conversations to read (and especially, if the conversations are not in English, translate).

> Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. **Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities**. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

Though, as I have noted before, contrary to what Shea says, this **by definition** serves to access content of **both** non-US and US persons: NSA is admitting that the selection criteria prioritizes calls from the US. And in the case of a FISC warrant it could easily be entirely US person content.

In other words, the use of the dragnet in conjunction with content warrants makes it more likely that US person content will be read.

Excluding bulk targets

Now, my analysis about the legal logic of all this starts to break down once the FISC approves bulk orders. In those programs — Protect America Act and FISA Amendments Act — analysts choose targets with no judicial oversight and the standard (because targets are assumed to be foreign) doesn't require probable cause. But the FISC recognized this. Starting with BR 07-16, the first order approved (on October 18, 2007) after the PAA until the extant PAA orders expired, the primary orders included language excluding PAA targets. Starting with 08-08, the first order approved (on October 18, 2007) after FAA until the present, the primary orders included language excluding FAA targets.

Of course, this raises a rather important question about what happened between the enactment of PAA on August 5, 2007 and the new order on October 18, 2007, or what happened between enactment of FAA on July 10, 2008 and the new order on August 19, 2008. Were analysts permitted to contact chain off of any of the targets they were tracking in the interim? Or did FISC pass supplemental orders in the interim?

The question should be of particular interest for Basaaly Moalin's lawyers. FBI has said they found his number through the phone dragnet two months before (they say only "October") they started wiretapping him around December 18, 2007. Which might place it before that language got included in the October 18, 2007 order. That's particularly significant given that al-Shabaab was not yet a designated Foreign Terrorist Organization when all this began.

Those funny overseas American warrants

Finally, there are two other curious details in the language in this section.

First, in addition to the language excluding anyone targeted off of Section 702 of FISA in that August 19, 2008 order, it (and subsequent orders) also excluded anyone targeted off of

Section 703 and 704, the warrants needed before wiretapping Americans overseas.

> Nor shall it apply to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

I don't pretend to understand why they excluded these warrants, which are supposed to be individual. There are problems with using the phone dragnet with foreign-to-foreign data, so that may be the reason FISC excluded these taps from automatic RAS treatment. But there's also a great deal of differing understanding — from civil liberties lawyers to the White House — about the limits to these two clauses. So who knows?!?

The pre-bulk collection bulk collection dockets?

Finally, in the dockets dated February 23 (?), 2007 and March 3 (?), 2007, the language excludes "telephone numbers under surveillance in Docket Number 06-2081."

> an NSA official. The preceding sentence shall not apply to telephone numbers under surveillance in Docket Number 06-2081.

And in the docket dated July 23 (?), 2007, it excludes "the telephone numbers under surveillance in Docket 07-449 or any renewal thereof."

> without approval of an NSA official. The preceding sentence shall not apply to the telephone numbers under surveillance in Docket Number 07-449 or any renewal thereof.

This language was replaced in the next order with the PAA language, suggesting they are also bulk collection.

These are notable for several reasons. We know — or think we know — that the FISC approved an early form of bulk collection — collection off the telecom switches — starting on January 10,

2007. It would make sense to exclude this bulk collection using the same logic for excluding the bulk collection under PAA or FAA: these weren't targets selected using probable cause.

These two passages would seem to suggest there were two different dockets using this formula. That makes sense too: in April or May 2007, a FISC judge rejected one of the applications, presenting the need for PAA.

But this would seem to say there was a bulk docket, 07-449, still active days before passage of the PAA.

In addition, the other docket number, 06-2081, would seem to suggest the bulk collection got approved sooner than we thought it did, sometime in 2006. The FISA Court approved 2176 FISA warrants in 2006, so this would be one of the later dockets in the year.

Now I could be totally wrong about what these two dockets represent. But they do raise questions about the pre-bulk collection bulk collection programs.

Update, 1/28/14: John Bates relied on 07-449 for the assumption that upstream content about a target was likely to involve foreign intelligence information. So these must be upstream collection targeted at content.

FREEDOM OF ASSOCIATION: FROM SIX DEGREES OF KEVIN BACON TO THREE DEGREES OF TERRY

STOP

One thing the July 24, 2004 Colleen Kollar-Kotelly opinion and the May 23, 2006 phone dragnet application reveal is that the government and the court barely considered the First Amendment Freedom of Association implications of the dragnets.

The Kollar-Kotelly opinion reveals the judge sent a letter asking the government about "First Amendment issues." (3) Way back on 57, she begins to consider First Amendment issues, but situates the in the querying of data, not the creation of a dragnet showing all relationships in the US.

> In this case, the initial acquisition of information is not directed at facilities used by particular individuals of investigative interest, but meta data concerning the communications of such individuals' [redacted]. Here, the legislative purpose is best effectuated at the querying state, since it will be at a point that an analyst queries the archived data that information concerning particular individuals will first be compiled and reviewed. Accordingly, the Court orders that NSA apply the following modification of its proposed criterion for querying the archived data: [redacted] will qualify as a seed [redacted] only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particularly known [redacted] is associated with [redacted] provided, however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that

> are protected by the First Amendment to the Constitution. For example, an e-mail account used by a U.S. person could not be a seed account if the only information thought to support the belief that the account is associated with [redacted] is that, in sermons or in postings on a web site, the U.S. person espoused jihadist rhetoric that fell short of "advocacy … directed to inciting or producing imminent lawless action and … likely to incite or produce such action." Brandnberg v. Ohio

By focusing on queries rather than collection, Kollar-Kotelly completely sidesteps the grave implications for forming databases of all the relationships in the US.

Then, 10 pages later, Kollar-Kotelly examines the First Amendment issues directly. She cites Reporters Committee for Freedom of the Press v. AT&T to lay out that in criminal investigations the government can get reporters' toll records. Predictably, she says that since this application is "in furtherance of the compelling national interest of identifying and tracking [redacted terrorist reference], it makes it an easier case. Then, finally, she cites Paton v. La Prade to distinguish this from an much less intrusive practice, mail covers.

> The court in Paton v. La Prade held that a mail cover on a dissident political organization violated the First Amendment because it was authorized under a regulation that was overbroad in its use of the undefined term "national security." In contrast, this pen register/trap and trace surveillance does not target a political group and is authorized pursuant to statute on the grounds of relevance to an investigation to protect against "international terrorism," a term defined at 50 U.S.C. § 1801(c). This definition has been upheld against a claim of First

> Amendment overbreadth. [citations omitted]

Of course, a mail cover is not automated and only affects the targeted party. This practice, by contrast, affects the targeted party (the selector) and anyone three hops out from him. Thus, even if those people are, in fact, a dissident organization (perhaps a conservative mosque), they in effect **become criminalized** by the association to someone only suspected — using the Terry Stop standard (the same used with stop-and-frisk) — of ties (but not even necessarily organizational ties) to terrorism.

Here's how it looks in translation, in the 2006 application:

> It bears emphasis that, given the types of analysis the NSA will perform, no information about a telephone number will ever be accessed or presented in an intelligible form to any person unless either (i) that telephone number has been in direct contact with a reasonably suspected terrorist-associated number or is linked to such a number through one or two intermediaries. (21)

So: queries require only a Terry Stop standard, and from that, mapping out everyone who is three degrees of association — **whose very association with the person should be protected by the First Amendment** — is fair game too.

Imagine if Ray Kelly had the authority to conduct an intrusive investigation into every single New Yorker who was three degrees of separation away from someone who had ever been stop-and-frisked. That's what we're talking about, only it happens in automated, secret fashion.

UNIVISION'S FOLLOW-UP QUESTION

Univision's Adriana Vargas just interviewed President Obama. After three questions about the immigration bill, she asked whether Obama would consider Ray Kelly to run Department of Homeland Security.

Obama, of course, was effusive about the idea of appointing Mr. Stop & Frisk to be in charge of the immigration system.

> Vargas: Mr. President, New York Commissioner Ray Kelly has been floated for the next DHS Secretary. What is your take on it?
>
> Obama: Well, Ray Kelly has obviously done an extraordinary job in New York and the federal government partners a lot with New York. Because obviously our concerns about terrorism oftentimes are focused on big city targets. And I think Ray Kelly is one of the best there is. So he's been an outstanding leader in New York. We've had an outstanding leader in Janet Napolitano at the Department of Homeland Security. It's a tough job. It's one of the toughest jobs in Washington. She's done an extraordinary job. We're sorry to see her go. But you know, we're going to have a bunch of strong candidates. Mr. Kelly might be very happy where he is. But if he's not I'd want to know about it. 'Cause you know, obviously he'd be very well qualified for the job.

Janet Napolitano? Outstanding leader.

Ray Kelly? Outstanding leader, according to Obama.

So Vargas then asked about a core DHS failure: Hurricane Sandy Recovery, where just a quarter

of families have gotten FEMA relief (about half of the relief funding remains unallocated).

Obama boasts about spending a quarter of the disaster relief funds, then shifts the subject to Shawn Donovan.

> AV: I have one last question regarding our geographical area of course and it's regarding the efforts of recovery after Sandy. Only a quarter of the families have received FEMA resources. What would be your message to those families among them obviously a lot of Latino families?
>
> PBO: Well, you know, we've distributed over $4 billion dollars since Sandy happened. $1.4 billion of that has been directly to families through FEMA. And we are continuing to not only try to get resources out. But also I've got a team headed up by Shaun Donovan, our Secretary of Housing and Urban Development to try to design a rebuilding process that strengthens these communities post-Sandy, so that if there are tragedies in the future they're in a stronger position than they were. But, you know, individual families it's always tough. Some may qualify for some assistance, but don't feel like they've gotten everything that they need. You know, we're doing as much as we can with the resources that we've been given from Congress. And we're in close communication with Governor Christie and Governor Cuomo and all the local municipalities to do everything we can to help businesses and families get back on their feet. And we're not going to stop until we get it done.

Obama's "outstanding" head of Homeland Security, of course, is ultimately responsible for Sandy recovery.

And that's apparently what he sees in Ray Kelly,

too.

HAVE CLAPPER, FEINSTEIN, AND ROGERS CONFUSED THE DISTINCT ISSUES OF SECTION 215 AND PRISM? OR ARE THEY INDISTINCT?

[youtube]hmw4G5q1OkE[/youtube]

Last year, when Pat Leahy tried to switch the FISA Amendments Act reauthorization to a 3 year extension instead of 5, which would have meant PATRIOT and FAA would be reconsidered together in 2015, the White House crafted a talking point claiming that would risk confusing the two provisions.

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

In the last week, the Guardian had one scoop pertaining to FAA (the PRISM program) and another to PATRIOT (the use of Section 215 to conduct dragnet collection of Americans' phone records).

Since then, almost everyone discussing the issues seems to have confused the two.

Including, at a minimum, Mike Rogers, as demonstrated by the video above. When Dianne Feinstein started explaining the Section 215 Verizon order, Mike Rogers interrupted to say that the program could not be targeted at

Americans. But of course the Section 215 order was explicitly limited to calls within the US, so he had to have been thinking of PRISM.

Then there what, on first glance, appears to be confusion on the part of journalists. I noted how Reuters' Rogers-related sources were clearly confused (or in possession of a time machine) when they made such claims, and NYT appeared to conflate the issues as well. Similarly, Andrea Mitchell took this exchange — which is clearly about Section 215 — and elsewhere reported that the law allowing NSA to wiretap Americans (which could be FISA or FAA) stopped the attack.

> ANDREA MITCHELL:
>
> At the same time, when Americans woke up and learned because of these leaks that every single telephone call in this United States, as well as elsewhere, but every call made by these telephone companies that they collect is archived, the numbers, just the numbers, and the duration of these calls. People were astounded by that. They had no idea. They felt invaded.
>
> JAMES CLAPPER:
>
> I understand that.
>
> [snip]
>
> A metaphor I think might be helpful for people to understand this is to think of a huge library with literally millions of volumes of books in it, an electronic library. Seventy percent of those books are on bookcases in the United States, meaning that the bulk of the of the world's infrastructure, communications infrastructure is in the United States.
>
> [snip]
>
> So the task for us in the interest of preserving security and preserving civil liberties and privacy is to be as precise as we possibly can be when we go

> in that library and look for the books that we need to open up and actually read.
>
> [snip]
>
> So when we pull out a book, based on its essentially is– electronic Dewey Decimal System, which is zeroes and ones, we have to be very precise about which book we're picking out. And if it's one that belongs to the– was put in there by an American citizen or a U.S. person.
>
> We ha– we are under strict court supervision and have to get stricter– and have to get permission to actually– actually look at that. So the notion that we're trolling through everyone's emails and voyeuristically reading them, or listening to everyone's phone calls is on its face absurd. We couldn't do it even if we wanted to. And I assure you, we don't want to.
>
> ANDREA MITCHELL:
>
> Why do you need every telephone number? Why is it such a broad vacuum cleaner approach?
>
> JAMES CLAPPER:
>
> Well, you have to start someplace. If– and over the years that this program has operated, we have refined it and tried to– to make it ever more precise and more disciplined as to which– which things we take out of the library. But you have to be in the– in the– in the chamber in order to be able to pick and choose those things that we need in the interest of protecting the country and gleaning information on terrorists who are plotting to kill Americans, to destroy our economy, and destroy our way of life.
>
> ANDREA MITCHELL:

> Can you give me any example where it actually prevented a terror plot?
>
> JAMES CLAPPER:
>
> Well, two cases that— come to mind, which are a little dated, but I think in the interest of this discourse, should be shared with the American people. They both occurred in 2009. One was the aborted plot to bomb the subway in New York City in the fall of 2009.
>
> And this all started with a communication from Pakistan to a U.S. person in Colorado. And that led to the identification of a cell in New York City who was bent on— make— a major explosion, bombing of the New York City subway. And a cell was rolled up, and in their apartment, we found backpacks with bombs.
>
> A second example, also occurring in 2009, involved— the— one of the— those involved, perpetrators of the Mumbai bombing in India, David Headley. And we aborted a plot against a Danish news publisher based on— the same kind of information. So those are two specific cases of uncovering plots through this mechanism that— prevented terrorist attacks.

What would seem to support the conclusion that everyone was just very confused is that, in his talking points on the two programs, Clapper claims three examples as successes for the use of PRISM, none of which is Zazi or Headley.

Now, the AP reports Clapper's office (which is fast losing credibility) has circulated talking points making the claim that PRISM helped nab Zazi.

> The Obama administration declassified a handful of details Tuesday that credited its PRISM Internet spying program with

> intercepting a key email that unraveled a 2009 terrorist plot in New York.
>
> The details, declassified by the director of national intelligence, were circulated on Capitol Hill as part of government efforts to tamp down criticism of two recently revealed National Security Agency surveillance programs.

But, as I suggested last year, the White House clearly wasn't concerned about us confusing our pretty little heads by conflating FAA and Section 215. Rather, it seemed then to want to hide the relationship between the dragnet collection of Americans calls and the direct access to Internet providers' data.

But Clapper and DiFi seem to hint at the relationship between them.

In her first comments about Section 215 (even before PRISM had broken) DiFi said this.

> The information goes into a database, the metadata, but cannot be accessed without what's called, and I quote, "reasonable, articulable suspicion" that the records are relevant and related to terrorist activity.

And in his talking points on 215, Clapper said this.

> By order of the FISC, the Government is prohibited from indiscriminately sifting through the telephony metadata acquired under the program. All information that is acquired under this program is subject to strict, court-imposed restrictions on review and handling. The court only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist

> organization.

This standard — reasonable suspicion that the records are relevant to or associated with a terrorist investigation (I'll come back to the terrorism issue in another post) — is not the 215 standard, because it requires reasonable suspicion. But it's not as high as a FISA warrant would be, which requires it to be more closely related than "relevant" to a terrorist investigation.

So what standard is this, and where did it come from?

Via email, Cato's Julian Sanchez hypothesizes that the FISA Court may have required the government apply the standard for Terry stops and ECPA to their ability to access US person data from the database.

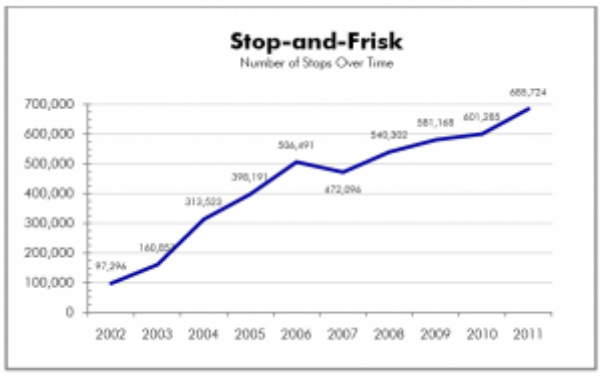
> It looks like they essentially imported the Terry stop-and-frisk standard, maybe by way of the ECPA "specific and articulable facts" standard in 18 USC 2703, as a post-collection constraint on QUERIES of the database, rather than its collection. That would comport with the DOD understanding that "acquisition" of a communication only occurs when it's actually processed into human-readable form and received by an analyst: They've concluded that the "relevance" test can be embedded in back end restrictions at the "query" phase where "acquisition" happens rather than the initial copying of the data. And they've used the ECPA/Terry standard as the test of relevance.

In other words, DiFi and Clapper's comments, in particular, and the underlying confusion that suggests there's a tie between PRISM and the Section 215 database generally, seem to suggest that the PRISM collection provides the evidence the government uses to get access to the

predominantly US person metadata to start seeing which Americans have 6 degrees of separation from the terrorists.

They're saying over and over again that they just can't go into the database willy nilly. Except they can access the PRISM data willynilly (including seeing the US person data) and use that to access a data of predominantly American records.

NYPD STOPPED 351,739 PEOPLE LAST YEAR FOR "FURTIVE MOVEMENTS"



There's been a good deal of reporting on this report the NYCLU released last week, but the report itself must be read to fully understand the gravity of the stop-and-frisk abuse in NYC.

Consider this chart, for example, showing that Mike Bloomberg has had even more success inflating stop-and-frisk numbers than he ever had inflating the stock market.

Then there's the stat that shows more young black men were stopped last year (168,126 stops of young black men) than reside in the city over all (158,406 total)—statistically, at least, every single young black man has been stopped.

Finally, though, there's the list of reasons cops gave for having stopped someone in the

first place—with “furtive movements” accounting for over half the stops, and “clothes commonly used in a crime” (does this mean hoodies?) cited in 31,555. What’s worse, cops only suspect a violent crime 10% of the time.

The cops frisked the person they stopped over half the time—purportedly because they suspected a weapon that might threaten the officer. Yet they found the weapon that justified the search less than 2% of the time—and weapons were more often found on white men who were stopped than blacks or LatinosIn December, Nicholas Peart wrote a devastating op-ed on what it has been like for him to mature under Bloomberg’s stop-and-frisk explosion, describing the four times he has been stopped and frisked.

> Last May, I was outside my apartment building on my way to the store when two police officers jumped out of an unmarked car and told me to stop and put my hands up against the wall. I complied. Without my permission, they removed my cellphone from my hand, and one of the officers reached into my pockets, and removed my wallet and keys. He looked through my wallet, then handcuffed me. The officers wanted to know if I had just come out of a particular building. No, I told them, I lived next door.
>
> One of the officers asked which of the keys they had removed from my pocket opened my apartment door. Then he entered my building and tried to get into my apartment with my key. My 18-year-old sister was inside with two of our younger siblings; later she told me she had no idea why the police were trying to get into our apartment and was terrified. She tried to call me, but because they had confiscated my phone, I couldn’t answer.
>
> Meanwhile, a white officer put me in the back of the police car. I was still

> handcuffed. The officer asked if I had any marijuana, and I said no. He removed and searched my shoes and patted down my socks. I asked why they were searching me, and he told me someone in my building complained that a person they believed fit my description had been ringing their bell. After the other officer returned from inside my apartment building, they opened the door to the police car, told me to get out, removed the handcuffs and simply drove off. I was deeply shaken.
>
> For young people in my neighborhood, getting stopped and frisked is a rite of passage. We expect the police to jump us at any moment. We know the rules: don't run and don't try to explain, because speaking up for yourself might get you arrested or worse. And we all feel the same way — degraded, harassed, violated and criminalized because we're black or Latino.

He ends this passage by asking, "Have I been stopped more than the average young black person?" And the ACLU report makes it clear that his experience is absolutely statistically normal for a young black man.

Which presumably means the result he describes—the fear, the degradation, the criminalization—are fairly typical as well.

This systematic humiliation of one segment of our society must not be tolerated.

HOW DO YOU PROFILE J.

EDGAR KELLY WITH ALMOST NO MENTION OF DOMESTIC SPYING?

In 1974, the NYT made history with a story that reported,

> An extensive investigation by the NYT has established that intelligence files on at least 10000 U.S. citizens were maintained by a special unit of the CIA

In 2005, the NYT again made history by exposing illegal domestic wiretapping.

Yet today's NYT managed to publish a 2,500-word story depicting Ray Kelly as some sort of J. Edgar Hoover figure with little mention—much less criticism—of the domestic spying Kelly's NYPD conducts on New Yorkers.

Much of the article vents complaints that Kelly has gotten remote, that he no longer cooks spaghetti for his officers. It buries an on the record quote from the president of the Sergeants Benevolent Association saying, "Among the rank-and-file, and even among the brass when I have talked to them, they are dying for a change" in the second-to-last paragraph.

But the five paragraphs addressing the rising number of scandals associated with the NYPD are striking for the way they deal with revelations of the domestic spying operation Kelly now oversees.

> After years of undeniable success, Commissioner Raymond W. Kelly is going through turbulent times, confronted with a steady drip of troublesome episodes. They include officers fixing traffic tickets, running guns and disparaging civilians on Facebook, and accusations that the Police Department encourages officers to question minorities on the streets indiscriminately. His younger

> son has been accused of rape, though he has not been charged and maintains his innocence. On Thursday, in an episode that Mr. Kelly said concerned him, an officer killed an 18-year-old drug suspect who was unarmed.
>
> [snip]
>
> He has built a counterterrorism machine with tentacles in 11 foreign cities, **irritating federal agencies. There has been no successful terrorist attack on his city while he has been commissioner. He has instead been engulfed** in the past year largely by familiar police corruption story lines, of human beings succumbing to greed or audacity.
>
> Over the past year, two officers charged with raping a woman were fired after being acquitted of rape but found guilty of official misconduct. A broad ticket-fixing scandal flared in the Bronx; when the accused officers were arraigned, hundreds of officers massed in protest, some denouncing Mr. Kelly. Eight current and former officers were charged with smuggling illegal guns. Narcotics detectives were accused of planting drugs on innocent civilians. An inspector needlessly pepper-sprayed four Occupy Wall Street protesters, invoking memories of the scrutiny and mass arrests of protesters during the 2004 Republican National Convention, and giving the nascent movement its first real prime-time moment.
>
> Civil rights advocates have assailed the department's expanded stops of minorities on the streets. Several officers denigrated West Indians on Facebook. **Muslims have denounced the monitoring of their lives, as Mr. Kelly has dispatched undercover officers and informants to find radicalized youth.**

> **This year began with the revelation that a film offensive to Muslims**, which included an interview with Mr. Kelly, had been shown to many officers.

The foreign intelligence "irritates federal agencies." "Muslims have denounced" domestic spying. An inaccurate and counterproductive film is "offensive to Muslims." The NYT seems anxious to dissociate itself from any criticism of the domestic spying, as if it's something only the targets should worry about, as if incorporating Islamophobia into police training has no negative effects.

Worse, the juxtaposition of the irritated federal agencies with the proclamation that there has been no successful attack seems to be an attempt to justify the domestic spying. Never mind that the two most serious attempted attacks—by Faisal Shahzad and Najibullah Zazi—were not discovered by Kelly's domestic spying. Never mind that the investigation into Zazi's plot was significantly harmed when the NYPD tipped Zazi off to it through his imam, whom the NYPD believed to be a reliable informant.

With the transition, "[h]e has instead been engulfed … by familiar police corruption story lines, of human beings succumbing to greed or audacity," the article logically distinguishes the domestic spying from the other things, the real scandals, according to the NYT.

And look at the one real reference to the domestic spying itself.

> Muslims have denounced the monitoring of their lives, as Mr. Kelly has dispatched undercover officers and informants to find radicalized youth.

Rather than stating what would be a fact—that undercover officers and informants are monitoring the lives of Muslim community members at large, it suggests that NYPD's intelligence

officers are selectively targeting “radicalized youth.” Which in turn delegitimizes the concerns of the Muslim leaders refusing to eat breakfast with Ray Kelly.

Look at their evidence for the assertion that Kelly “has dispatched undercover officers and informants to find radicalized youth.” A 2006 article reporting on revelations of NYPD infiltration of the Islamic Society of Bay Ridge made in the course of the Shahawar Matin Siraj trial. The article claims to be unable to determine the real extent of the spying, so instead includes credulously repeated quotes insisting the NYPD is not engaging in spying at mosques.

> The police would provide no details about the unit and how it operates beyond what came out at the trial. So its scope, the guidelines under which it works and its successes and failures, beyond Mr. Siraj’s conviction, could not be immediately determined.
>
> [snip]
>
> During the trial, a senior police official acknowledged that mosques had at one time been a focus of the department’s efforts, but he said that investigators had significantly broadened their scope since then.
>
> “We don’t investigate mosques, we investigate people,” the official said. “We’re not in every mosque — that’s not where we need to be. That’s Intel 101. We’re in the graduate program. The bad guys aren’t hanging around the water cooler after Friday prayers anymore.”

My favorite part of the reliance on this article is the date: May 28, 2006, just 13 days after (we now know) a document **addressed to Kelly himself** described plans for further infiltration of mosques, two by name, as well as the 16 other Shia mosques and cultural centers in the

vicinity of NYC (or rather, as the AP reported, 15 other Shia sites and one erroneously labeled as such).

How do you write a profile of Ray Kelly without noting that he has been personally overseeing broad-based domestic spying based on religion?

One way you do that is by making no mention of the AP series exposing these things, or even the NYT's own Michael Powell reporting that the NYPD targets not "radicalized youth" but "preradicalized" Muslim men.

> The Police Department was open about its ambitions in a 2007 report, "Radicalization in the West: The Homegrown Threat." The authors claim to detect a path from "preradicalization" to "jihadization," driven by a fundamentalist ideology "proliferating in Western democracies at a logarithmic rate."
>
> The department is intent on finding young Muslim men in a "preradicalization" state before they embark on jihad.

By simply ignoring the mounting evidence of the abuses included in the NYPD's domestic spying program, you can—as the NYT does—dismiss it as the concern of federal agencies or those being targeted.

In the past, the NYT treated abusive domestic spying as important news. When it happens to scary brown people in its own city, however, the NYT appears to treat it as the irrational whining of purportedly legitimately targeted groups.

NYDN: CENSUS NOW MAPPING YOUR BACK HALLWAYS

A bunch of leaders in NYC's Muslim community have declined Mayor Mike Bloomberg's invitation to an interfaith breakfast because of the racial profiling done by the NYPD's intelligence division.

The move is interesting for the press it has generated—which in turn, has also (presumably, as designed) focused new attention on the racial profiling itself

It's interesting, too, for the obnoxious editorial written in response from the NYDN. Along with lecturing these Muslim leaders about what invitations they should accept, the NYDN claims that the NYPD had done no more than map out census data.

> The plain and salutary fact is that the NYPD's counterterrorism unit has done no more than use census data to develop a portrait of Muslim New York and then follow leads, some sent the city's way from abroad via the CIA, when they demanded investigation.
>
> Many a plot has been disrupted by this type of perfectly proper nonintrusive vigiliance.

I find the claim that this all came from census data alarming, given that the NYPD has actually cased out a bunch of Middle Eastern restaurants in the city, including details such as what back passages the restaurants have, as in these details about the Eastern Nights Cafe.

> The restaurant consists of two stores next to each other, connected to each other from the back of the store. The restaurant also has a back yard. The restaurant has access to the basement; the access door is located on the far right of the store.

Note, too, that while NYDN might be speaking generally about the "many a plot" that has been disrupted by mapping the back hallways of NY restaurants, this surveillance has not only disrupted primarily aspirational plots, but it damaged the FBI investigation into the real plot Najibullah Zazi had planned, because one of the NYPD's own informants tipped the Zazis off to the investigation.

And the invitation declination is interesting, finally, for the way the Muslim leaders framed this issue—as part of a larger choice on the part of the NYPD to neglect law enforcement while it engages in civil rights abuses not just of Muslims, but of people of color and Occupy Wall Street protestors.

> Mayor Bloomberg, the extent of these civil rights violations is astonishing, yet instead of calling for accountability and the rule of law, you have thus far defended the NYPD's misconduct. We, on the other hand, believe that such measures threaten the rights of all Americans, and deepen mistrust between our communities and law enforcement. We are not alone in our belief. Many New Yorkers continue to express a variety of concerns centered on a lack of law enforcement accountability in our city, from stop

> and frisk procedures in African American and Spanish-speaking communities, to the tactics used in the evacuation of Zuccotti Park.

That’s really what the NYPD surveillance is about: prioritizing the profiling of an entire community (even while periodically and repeatedly stopping and frisking totally innocent people of color), rather than investigating and solving actual crimes.