DID MUELLER'S TEAM DECIDE THEY NO LONGER NEED MANAFORT TO FLIP?

Given TS Ellis' focus on the probability Mueller charged Paul Manafort with tax charges only to get him flip in the investigation against Trump, I find it notable that Mueller's EDVA brief did not include language the DC brief did on doing just that.

---

702 REAUTHORIZATION BILL: WHY A BACK DOOR FIX FOR CRIMINAL SEARCHES IS MEANINGLESS

Because of the way FBI uses assessments to decide whether someone might make a good foreign intelligence asset, the back door search fix is meaningless, because virtually any back door search can be deemed a foreign intelligence search.

MAYBE FBI HAS LOST TRACK OF WHO THE

INFORMANTS ARE?

Here are all the informants and undercover employees listed in the criminal complaint against Erick Hendricks, who was arrested for conspiring to materially support ISIL in relation to the Garland, TX attack:

- CHS-1: a paid informant for the last year and a half with a criminal record of fraud and forgery who has not (yet?) received sentencing benefits for his cooperation; he met with Hendricks in Baltimore.
- CHS2: a paid informant for the last 4 years with no known criminal history; he posed as someone wanting to join ISIL.
- CHS-3: a paid informant for the last 4 and a half years with no known criminal history; Hendricks instructed CHS-3 to assess UCE-1 for recruitment.
- CHS-4: a paid informant for the last 4 years with no known criminal history; Hendricks provided him with jihadist propaganda on social media. He also met with Hendricks in Baltimore, at a later date.
- UCE-1: an undercover officer had conversations directly with Hendricks that mirrored

> those Hendricks had with a cooperating witness. UCE-1 also incited and then was present for the Garland attack.

Not mentioned at all in this narrative is the role played by Joshua Goldberg, a Jewish guy who adopted many avatars online to incite all kinds of violence, including, under the name of Australi Witness, Garland. In December Goldberg was deemed incompetent to stand trial, though in June it was decided with more treatment he might become competent enough to stand trial, so they're going to check again in four months.

So, the cell that committed the Garland attack consisted of the two now-dead perpetrators, four informants, an undercover FBI officer, a mentally ill troll, and Hendricks.

Only now, Hendricks claims he was an informant too!

> Hendricks claims to have been a paid informant of the FBI since 2009 who helped the agency identify potential terrorists. Code name: "Ahkie," a variation of the Muslim term for "brother."
>
> He also claims to have been an outspoken and longtime opponent of radical Islam.
>
> "I have publicly, privately and consistently denounced Al-Qaeda, ISIS and all extremist groups," Hendricks said in a statement that Lisa Woods says her son dictated during a Wednesday phone call from the jail.
>
> "I am baffled as to why the FBI (is) accusing me of terrorist ties."
>
> [snip]
>
> In his statement, Hendricks says the FBI first made contact with him in 2009,

> when as Mustafa Abu Maryam, Hendricks was the youth coordinator of the Islamic Circle of North America Center in Alexandria, Va.
>
> [snip]
>
> In his jail statement, Hendricks says he was recruited in 2009 by an FBI agent named David to help identify potential terrorists. In 2010, after Hendricks had moved to Columbia, he says he worked with another FBI agent named Steve. Altogether, Hendricks claims to have developed "at least a half-dozen" cases against extremists.

Has the FBI simply lost track of who are real and who are the people it is paying to play a role? Or is it possible someone from another agency, claiming to be FBI, recruited Hendricks (don't laugh! That's one potential explanation for Anwar al-Awlaki's curious ties to US law enforcement, a story that wends its way through a related mosque in VA)?

Sure, maybe Hendricks is making all this up (at the very least, it may necessitate the BoP to protect him in prison since he has now publicly claimed to be a narc). But FBI's network of informants sure is getting confusing.

FORMER TOP HOLDER AIDE SAYS BACK DOOR SEARCHES VIOLATE FOURTH AMENDMENT;

FISC JUDGE THOMAS HOGAN DOESN'T CARE

My apologies to Amy Jeffress.

When I first realized that FISA Court Presiding Judge Thomas Hogan picked her to serve as amicus for the review of the yearly 702 certifications last year, I complained that she, not Marc Zwillinger, got selected (the pick was made in August, but Jeffress would later be picked as one of the standing amicus curiae, along with Zwillinger). After all, Zwillinger has already argued that PRISM (then authorized by Protect America Act) was unconstitutional when he represented Yahoo in its challenge of the program. He's got experience making this precise argument. Plus, Jeffress not only is a long-time national security prosecutor and former top Eric Holder aide, but she has been involved in some actions designed to protect the Executive. I still think Zwillinger might have done a better job. But Jeffress nevertheless made what appears to be a vigorous, though unsuccessful, argument that FBI's back door searches of US person data are unconstitutional.

A former top DOJ lawyer believes FBI's back door queries are unconstitutional

But it says a lot that Jeffress — someone who narrowly missed being picked as Assistant Attorney General for National Security and who presumably got at least some visibility on back door searches when working with Holder — argued that FBI's warrantless back door searches of communications collected under Section 702 is unconstitutional. (I presume it would be unethical for Jeffress to use information learned while counseling Holder in this proceeding, which might have put her in an interesting position of knowing more than she

could say.)

Sadly, Hogan didn't care. Worse, his argument for not caring doesn't make sense. As I'll note, not only did Hogan pick a less than optimal person to make this argument, but he may have narrowly scoped her input, which may have prevented her from raising evidence *in Hogan's own opinion* that his legal conclusion was problematic.

To be clear, Jeffress was no flaming hippie. She found no problem with the NSA and CIA practice of back door searches, concluding, "that the NSA and CIA minimization procedures are sufficient to ensure that the use of U.S. person identifiers for th[e] purpose of [querying Section 702-acquired information] complies with the statutory requirements of Section 702 and with the Fourth Amendment." But she did find the FBI practice problematic.

Jeffress' amicus brief included at least 10 pages of discussion of her concerns with the practice, though ODNI did not release her brief and Hogan cited very limited bits of it. She argued, "the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes" and said because the queries could do so they "go far beyond the purpose for which the Section 702-acquired information is collected in permitting queries that are unrelated to national security."

To dismiss Jeffress' arguments, Hogan does several things. He,

- Notes the statute requires foreign intelligence just be "a significant purpose" of the collection, and points back to the 2002 *In Re Sealed Case* FISCR decision interpreting the "significant purpose" language added in the

PATRIOT Act to permit the use of traditional FISA information for prosecutions
- Cites the FISA minimization procedure language that "allow[s] for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed"
- Dismisses a former top DOJ official's concerns about the use of FISA data for non-national security crimes as "hypothetical"
- Doesn't address — at all — language in the FBI minimization procedures that permits querying of data for assessments and other unspecified uses
- Invests a lot of faith in FBI's access and training requirements that later parts of his opinion undermine

There are several problems with his argument.

In Re Sealed Case ties "significant purpose" to the target of an interception

First, Hogan extends the scope of what the FISA Court of Review interpreted the term "significant purpose," which got added to traditional FISA in the PATRIOT Act and then

adopted in FISA Amendments Act.

Hogan cites the FISCR decision in *In Re Sealed Case* to suggest it authorized the use of information against non-targets of surveillance. He does so by putting the court's ultimate decision after caveats it uses to modify that. "The Court of Review concluded that it would be an "anomalous reading" of the "significant purpose" language of 50 U.S.C. § 1804(a)(6)(B) to allow the use of electronic surveillance in such a case. See id. at 736. The Court nevertheless stressed, however, that "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution that it satisfies the significant purpose test."

But that's not what FISCR found. Here's how that reads in the original, with Hogan's citations emphasized.

> On the one hand, Congress did not amend the definition of foreign intelligence information which, we have explained, includes evidence of foreign intelligence crimes. On the other hand, Congress accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test. Nevertheless, it is our task to do our best to read the statute to honor congressional intent. The better reading, it seems to us, excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution. We therefore reject the government's argument to the contrary. Yet this may not make much practical difference. Because, as the government points out, when it commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent (whatever may be the subjective intent of the investigators or lawyers who initiate an

> investigation). So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.
>
> The important point is—and here we agree with the government—the Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the application's purpose articulates a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.
>
> The government claims that even prosecutions of *non*-foreign intelligence crimes are consistent with a purpose of gaining foreign intelligence information so long as the government's objective is to stop espionage or terrorism by putting an agent of a foreign power in prison. That interpretation transgresses the original FISA. It will be recalled that Congress intended section 1804(a)(7)(B) to prevent the government from targeting a foreign agent when its "true purpose" was to gain non-foreign intelligence information—such as evidence of ordinary crimes or scandals. See supra at p.14. (If the government

> inadvertently came upon evidence of ordinary crimes, FISA provided for the transmission of that evidence to the proper authority. 50 U.S.C. § 1801(h)(3).) It can be argued, however, that by providing that an application is to be granted if the government has only a "significant purpose" of gaining foreign intelligence information, the Patriot Act allows the government to have a primary objective of prosecuting an agent for a non-foreign intelligence crime. Yet we think that would be an anomalous reading of the amendment. For we see not the slightest indication that Congress meant to give that power to the Executive Branch. Accordingly, the manifestation of such a purpose, it seems to us, would continue to disqualify an application. That is not to deny that ordinary crimes might be inextricably intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself. But the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.

Hogan ignores three key parts of this passage. First, FISCR's decision only envisions the use of evidence against the *target* of the surveillance, not against his interlocutors, to in some way neutralize him. Any US person information collected and retained under 702 is, by definition, not the targeted person (whereas he or she might be in a traditional FISA order). Furthermore, FBI's queries of information collected under 702 will find and use information that has nothing to do with putting foreign agents in prison — that is, to "investigate wholly unrelated ordinary

crimes," which FISCR prohibited. Finally, by searching data that may be years old for evidence of a crime, FBI is, in effect, "gaining evidence of past criminal conduct" — itself prohibited by FISCR — of someone who isn't even the target of the surveillance.

Hogan only treats querying for criminal purposes

Having, in my opinion, expanded on what FISCR authorized back in 2002, Hogan then ignores several parts of what FBI querying permits.

Here's (some of) the language FBI added to its minimization procedures, at the suggestion of PCLOB, to finally, after 8 years, fully disclose what it was doing to the FISC.

> It is a routine and encouraged practice for FBI to query databases containing lawfully acquired information, including FISA-acquired information, in furtherance of the FBI's authorized intelligence and law enforcement activities, such as assessments, investigations and intelligence collection. Section III.D governs the conduct of such queries. Examples of such queries include, but are not limited to, queries reasonably designed to identify foreign intelligence information or evidence of a crime related to an ongoing authorized investigation or reasonably designed queries conducted by FBI personnel in making an initial decision to open an assessment concerning a threat to national security, the prevention or protection against a Federal crime, or the collection of foreign intelligence, as authorized by the Attorney General Guidelines. These examples are illustrative and neither expand nor restrict the scope of the queries authorized in the language above.

This language makes clear FBI may do back door searches for:

- To identify foreign intelligence information
- To identify evidence of a crime related to an ongoing investigation
- To decide whether to open an assessment concerning a threat to national security, the prevention or protection against a Federal crime, or the collection of foreign intelligence
- Other things, because FBI's use of such queries "are not limited to" these uses

Given Hogan's stingy citations from Jeffress' brief, it's unclear how much of these things she addressed (or whether she was permitted to introduce knowledge gained from having worked closely with Eric Holder when these back door searches were being formalized).

But he only treats her objection that FISC cannot be used "to investigate wholly unrelated ordinary crimes."

And his treatment of that is pretty unconvincing. Indeed, at times Hogan's rationalizations read like he's trying to convince himself. He cites, without quoting, these two statements from the PCLOB 702 report (the first is from the report itself; the second is from Rachel Brand and Elisabeth Collins Cook's separate statement).

> Anecdotally, the FBI has advised the Board that it is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from

> the query against the Section 702–acquired data.
>
> [snip]
>
> We are unaware of any instance in which a database query in an investigation of a non–foreign intelligence crime resulted in a "hit" on 702 information, much less a situation in which such information was used to further such an investigation or prosecution.

Because FBI didn't track these queries before this ruling, *it actually doesn't know* whether any query has resulted in such a hit, and neither statement claims to be proof it never happened. From that absence of evidence, however, Hogan calls the risk "remote, if not entirely theoretical," then treats it as a "hypothetical problem."

Worse, Hogan presumably has reason to know the possibility is not remote at all. After all, Hogan himself authorized an expansion of FBI's minimization procedures in 2014 permitting FBI to share 702 information with the National Center on Missing and Exploited Children, which is a pretty clear indication that FBI planned to use 702 data to investigate kiddie porn. Kiddie porn is a serious crime. But it is not, usually, a national security one (except insofar as the government now treats some Transnational Crime Organizations like it does terrorist groups). Nowhere in his discussion does Hogan explain why 702 information should be used to investigate kiddie porn, or what FBI's clear intent to do so means for the Fourth Amendment analysis of back door searches on US persons.

Hogan's okay with what he calls a theoretical possibility a non-national security crime might be investigated using back door searches, though, based on this equally theoretical example — offered by the government at the hearing — that FBI will stumble on a foreign terrorist tie when investigating some kind of

common criminal plot.

> A query designed to find and extract data regarding a [redacted] plot, for example, might reveal a previously unknown connection to persons believed to be funding terrorist operations on behalf of [redacted]

But what this suggestion means is that alleged terrorists with ties to a foreign organization may be investigated with information collected with less than a warrant standard. By contrast, if the FBI were to investigate, say, Robert Dear (the Colorado Springs Planned Parenthood killer, who long hailed the actions of other anti-choice terrorists and sometimes communicated with them) or the Malheur Refugee occupiers, with their ties to groups that have threatened the government, FBI would be less likely to find data showing such ties, because to actually have collected it in the past, FBI would have needed to reach a probable cause standard not required for FISA, much less 702. Yet there's no reason to believe Islamic extremists here in the US are a bigger threat than other kinds of terrorists. Moreover, to treat white Christian terrorists with a probable cause standard while treating Muslim terrorists with a NSA targeting standard is patently unequal treatment before the law, especially when you consider how FBI might turn conversations with radicals into reason to set up a sting against a person.

Hogan ignores other potential queries under FBI's minimization procedures

As noted, there are two other things clearly permitted in FBI's new minimization procedures language on which Hogan is completely silent: to decide whether to open an assessment, or other things not laid out in the minimization procedures.

One of the known uses of such queries is tied quite closely to the question of whether 702 data should be used to investigate common crimes, and it's one Hogan tacitly invokes when he invokes *In Re Sealed* case. As I have noted in the past, during the FISCR hearing in that case, then Solicitor General Ted Olson argued that if the government obtained evidence of rape using a FISA wiretap, they might then use such information to coerce the rapist in question to become an informant.

> OLSON: And it seems to me, if anything, it illustrates the position that we're taking about here. That, Judge Silberman, makes it clear that to the extent a FISA-approved surveillance uncovers information that's totally unrelated – let's say, that a person who is under surveillance has also engaged in some illegal conduct, cheating –
>
> JUDGE LEAVY: Income tax.
>
> SOLICITOR GENERAL OLSON: Income tax. What we keep going back to is practically all of this information might in some ways relate to the planning of a terrorist act or facilitation of it.
>
> JUDGE SILBERMAN: Try rape. That's unlikely to have a foreign intelligence component.
>
> SOLICITOR GENERAL OLSON: It's unlikely, but you could go to that individual and say we've got this information and we're prosecuting and you might be able to help us. I don't want to foreclose that.
>
> JUDGE SILBERMAN: It's a stretch.
>
> SOLICITOR GENERAL OLSON: It is a stretch but it's not impossible either. [my emphasis]

The FBI admits it uses assessments to find informants. Doing so might easily qualify under

"the decision to open an assessment." And, especially if the FBI were using something embarrassing but not illegal (say, evidence that an Imam were engaged in an extramarital affair) to coerce a person to spy, that would have enormous implications under the Fourth Amendment.

Similarly, FBI admits it uses assessments to engage in domestic profiling — such as to map out the Somali community in Saint Paul. I could see the FBI using communications between people writing from IP addresses in certain cities to targets of interest in Somalia to decide that such profiling — of entire communities! — was worthwhile. But Hogan doesn't deal with FBI's use of 702 queries for assessments at all. It's a clear part of their minimization procedures, and he doesn't include it, at all, in his Fourth Amendment analysis.

Which, of course, leaves that "such queries include, but are not limited to," language in FBI's minimization procedures (which reveals the practice is even more invasive than described in the PCLOB report). What is FBI doing with this data? And why, once again, is Hogan approving minimization procedures that don't lay out how this domestic surveillance is being used?

After relying on protections in FBI's minimization procedures to deem FBI's queries constitutional, Hogan then lays out two ways FBI's minimization procedures aren't being followed

As noted, there's one more thing Hogan relies on to find FBI's querying process constitutional. He cites the restrictions in the FBI's minimization procedures to suggest the protections are adequate. "With respect to the

intrusiveness of the querying process, the FBI Minimization Procedures impose substantial restrictions on the use and dissemination of information derived from queries."

In an few cases, Hogan cites what Jeffress found problematic — that even people without training in 702 data can access it on a one-time basis to assess the information — as proof of its control. "In 'very rare' circumstances," he cites the hearing, "FBI personnel who are not trained for and do not have access to Section 702-acquired information may view the results of a query solely to aid in the determination of whether the information constitutes foreign intelligence information or evidence of a crime."

Yet the second half of Hogan's opinion — dealing with 702 as implemented, including the numerous violations reported in the year leading up to these certifications — even further undermines Hogan claim that minimization procedures make the queries acceptable. Two of the violations Hogan describes pertain to FBI minimization procedures not being enforced. For example, in his description of the multiple cases — documented in 6 different compliance reports over the previous year and what appear to be at least three more in 2014 — where FBI did not meet its own (wholly inadequate, given that protection is focused primarily on indicted defendants) minimization procedures designed to protect attorney-client communications, Hogan judged, "FBI case agents are generally aware of the requirement for a review team when a Section 702 target is charged with a federal crime, but they are confused about the specific requirements of the FBI Minimization Procedures." He does so while describing a situation that, by asking agents whether a target might be indicted in the future, might encourage agents to delay indictment so as to delay the time when attorney-client communications would become subject to the taint team.

More troubling is an almost entirely redacted violation pertaining to failure of access controls to raw 702 data. Hogan introduces a two page, entirely redacted discussion about this problem by noting that FBI's minimization procedures grant access to raw 702 data "'permitting access … only by individuals who require access in order to perform their job duties'" and also "requires users with access to raw FISA-acquired information to receive training on the minimization procedures." That introduction only makes sense if the redacted two pages explain that FBI is not meeting those procedures. And it comes a year after Hogan appears to have learned of similar problems with access controls on ad hoc FBI databases created from 702 data. Less than ten pages after having found FBI's querying process constitutional because of access limits and training required to use this data, then, Hogan lays out how FBI access controls don't work and agents remain "confused" even after being trained on the minimization procedures.

Plus, throughout the discussion of compliance problems (including more pertaining to NSA), there's no mention of Jeffress' involvement (~~although the attorney-client review team problems were discussed at a hearing that she also attended~~ Correction: that hearing was on a different date than the one she participated in). It's unclear whether Hogan permitted Jeffress to learn of these violations (he determines what she needs to do her job, after all), and if she didn't have access to it, it would have prevented her from showing why the FBI's minimization procedures aren't adequate to protect Fourth Amendment rights.

Hogan's easily gamed reporting requirement

Hogan doesn't leave FBI's querying process entirely untouched. He imposed a requirement that FBI "submit in writing a report concerning each instance … in which FBI personnel receive

and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information." Such reporting, if required indefinitely, is worthwhile — and should have been required by Congress under USA Freedom Act.

But FBI can and presumably will game this information in two ways. First, FBI's querying system can be set such that, even if someone has access to 702 data, they can run a query that will flag a hit in 702 data but won't actually show the data underlying that positive return. This provides one way for 702-cleared people to learn that such information is in such a collection and — if they want the data without having to report it — may be able to obtain it another way. It is distinctly possible that once NSA shares EO 12333 data directly with FBI, for example, the same data will be redundantly available from that in such a way that would not need to be reported to FISC. (NSA used this arbitrage method after the 2009 problems with PATRIOT-authorized database collections.)

Plus, such reporting depends on the meaning of foreign intelligence information as defined under the Attorney General Guidelines.

> FOREIGN INTELLIGENCE: information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.

It would be relatively easy for FBI to decide that any conversation with a foreign person constituted foreign intelligence, and in so doing count even queries on US persons to identify criminal evidence as foreign intelligence information and therefore exempt from the reporting guidance. Certainly, the kinds of queries that might lead the FBI to profile St. Paul's Somali community could be

considered a measure of Somali activities in that community. Similarly, FBI might claim the search for informants who know those in a mosque with close ties overseas could be treated as the pursuit of information on foreign activities in US mosques.

Hogan imposed a worthwhile new reporting requirement. But that's still a very far cry from conducing a fair assessment of whether FBI's back door searches are constitutional.

NSA'S DRAGNET FAILED TO "CORRELATE" DAVID HEADLEY'S IDENTITY, ONE OF ITS CORE FUNCTIONS

In a piece on the GCHQ and NSA failure to identify David Headley's role in the Mumbai terrorist attack, ProPublica quotes former CIA officer Charles Faddis on the value of bulk surveillance.

> "I'm not saying that the capacity to intercept the communications is not valuable," said Charles (Sam) Faddis, a former C.I.A. counterterror chief. "Clearly that's valuable." Nonetheless, he added, it is a mistake to rely heavily on bulk surveillance programs in isolation.
>
> "You're going to waste a lot of money, you're going to waste a lot of time," Faddis said. "At the end, you're going have very little to show for it."

The article as a whole demonstrates that in a manner I'm fairly shocked about. The NSA failed to recognize what it had in intelligence collected on Headley's role in the attack *even after the attack* because they hadn't correlated his *known birth name* with the name he adopted in the US.

> Headley represents another potential stream of intelligence that could have made a difference before Mumbai. He is serving 35 years in prison for his role. He was a Pakistani-American son of privilege who became a heroin addict, drug smuggler and DEA informant, then an Islamic terrorist and Pakistani spy, and finally, a prize witness for U.S. prosecutors.
>
> In recounting that odyssey, we previously explored half a dozen missed opportunities by U.S. law enforcement to pursue tips from Headley's associates about his terrorist activity. New reporting and analysis traces Headley's trail of suspicious electronic communications as he did reconnaissance missions under the direction of Lashkar and Pakistan's Inter-Services Intelligence Directorate (ISI).
>
> Headley discussed targets, expressed extremist sentiments and raised other red flags in often brazen emails, texts and phone calls to his handlers, one of whom worked closely on the plot with Shah, the Lashkar communications chief targeted by the British.
>
> U.S. intelligence officials disclosed to me for the first time that, after the attacks, intensified N.S.A. monitoring of Pakistan did scoop up some of Headley's suspicious emails. But analysts did not realize he was a U.S.-based terrorist involved in the Mumbai attacks who was at work on a new plot against Denmark, officials admitted.

> The sheer volume of data and his use of multiple email addresses and his original name, Daood Gilani, posed obstacles, U.S. intelligence officials said. To perfect his cover as an American businessman, Headley had legally changed his name in 2006.
>
> "They detected a guy named 'Gilani' writing to bad guys in Pakistan, communicating with terror and ISI nodes," a senior U.S. intelligence official said. "He wrote also in fluent Urdu, which drew interest. Linking 'Gilani' to 'Headley' took a long time. The N.S.A. was looking at those emails post-Mumbai. It was not clear to them who he was."

As I've explained, one of the things NSA does with all its data is to "correlate" selectors, so that it maps a picture of all the Internet and telecom (and brick and mortar, where they have HUMINT) activities of a person using the multiple identities that have become common in this day and age. This is a core function of the NSA's dragnets, and it works automatically on EO 12333 data (and worked automatically on domestically-collected phone and — probably — Internet metadata until 2009).

When you think about it, there are some easy ways of matching online identities (going to a provider, mapping some IP addresses). And even the matching of "burner" IDs can be done with 94% accuracy, at least within AT&T's system, according to AT&T's own claims.

The NSA says they didn't do so here because Headley had changed his name.

Headley, recall, was a DEA informant. Which means, unless these intelligence agencies are far more incompetent than I believe they are, this information was sitting in a government file somewhere: "Daood Gilani, the name of a known Urdu-fluent informant DEA sent

off to Pakistan to hang out with baddies = David Headley." Unless Headley adopted the new name precisely because he knew it would serve to throw the IC off his trail.

And yet … NSA claims it could not, and did not, correlate those two identities and as a result didn't even realize Headley was involved in the Mumbai bombing even after the attack.

Notably, they claim they did not do so because of the "sheer volume of data."

In short, according to the NSA's now operative story (you should click through to read the flaccid apologies the IC offered up for lying about the value of Sections 215 and 702 in catching Headley), the NSA's dragnet failed at one of its core functions because it is drowning in data.

FBI'S PREVENTATIVE ROLE: HYGIENE FOR CORPORATIONS, SPIES FOR MUSLIMS

I'm still deep in this 9/11 Follow-up Report FBI, which Jim Comey and now-retired Congressman Frank Wolf had done last year and which released the unsurprising topline conclusion that Jim Comey needs to have more power, released earlier this week.

About the only conclusion in the report that Comey disagreed with — per this Josh Gerstein report — is that it should get out of the business of Countering Violent Extremism.

> Comey said he agreed with many of the report's recommendations, but he

> challenged the proposal that the FBI leave counter-extremism work to other agencies.
>
> "I respectfully disagree with the review commission," the director said. "It should not be focused on messages about faith it should not be socially focused, but we have an expertise … I have these people who spend all day long thinking dark thoughts and doing research at Quantico, my Behavioral Analysis Unit. They have an incredibly important role to play in countering violent extremism."

Here's what the report had to say about FBI and CVE (note, this is a profoundly ahistorical take on the serial efforts to CVE, but that's just one of many analytical problems with this report).

> The FBI, like DHS, NCTC, and other agencies, has made an admirable effort to counter violent extremism (CVE) as mandated in the White House's December 2011 strategy, Empowering Local Partners to Prevent Violent Extremism in the United States. In January 2012, the FBI established the Countering Violent Extremism Office (CVEO) under the National Security Branch.322 The CVEO was re-aligned in January 2013 to CTD's Domestic Terrorism Operations Section, under the National JTTF, to better leverage the collaborative participation of the dozens of participating agencies in FBI's CVE efforts.323 Yet, even within FBI, there is a misperception by some that CVE efforts are the same as FBI's community outreach efforts. Many field offices remain unaware of the CVE resources available through the CVEO.324 Because the field offices have to own and integrate the CVE portfolio without the benefit of additional resources from FBI Headquarters, there is

> understandably inconsistent implementation. The Review Commission, through interviews and meetings, heard doubts expressed by FBI personnel and its partners regarding the FBI's central role in the CVE program. The implementation had been inconsistent and confusing within the FBI, to outside partners, and to local communities.325 The CVEO's current limited budget and fundamental law enforcement and intelligence responsibilities do not make it an appropriate vehicle for the social and prevention role in the CVE mission. Such initiatives are best undertaken by other government agencies. The Review Commission recommends that the primary social and prevention responsibilities for the CVE mission should be transferred from the FBI to DHS or distributed among other agencies more directly involved with community interaction.
>
> [snip]
>
> (U) Recommendation 6: The Review Commission recommends that the primary social and prevention responsibilities for the CVE mission should be transferred from the FBI to DHS or distributed among other agencies more directly involved with community interaction.

For what it's worth, Muslim communities increasingly agree that the FBI — and the federal government generally — should not be in the business of CVE. But that's largely because the government approaches it with the same view Comey does: by thinking immediately of his analysts thinking dark thoughts at Quantico. So if some agency that had credibility — if some agency had credibility — at diverting youth (of all faiths) who might otherwise get caught in an FBI sting, I could support it moving someplace else, but I'm skeptical DHS or any other

existing federal agency is that agency right now.

While the Review doesn't say explicitly in this section what it wants the FBI to be doing instead of CVE, elsewhere it emphasizes that it wants the FBI to do more racial profiling (AKA "domain awareness") and run more informants. Thus, I think it fair to argue that the Ed Meese-led panel thinks the FBI should spy on Muslims, not reach out to them. Occupation-style federal intelligence gathering, not community based.

Which is why I think this approach to Muslim communities should be compared directly with the Review's approach with corporations. The same report that says FBI should not be in the business of CVE – which done properly is outreach to at-risk communities – says that it should accelerate and increase its funding for its outreach to the private sector.

> (U) Recommendation 5: The Review Commission recommends that the FBI enhance and accelerate its outreach to the private sector.
>
> - *(U) The FBI should work with Congress to develop legislation that facilitates private companies' communication and collaboration and work with the US Government in countering cyber threats.*
> - *(U) The FBI should play a prominent role in coordinating with the private sector, which the Review Commission believes will require a*

> *full-time position for a qualified special agent in the relevant field offices, as well as existing oversight at Headquarters.*

Indeed, in a paragraph explaining why the FBI should add more private sector liaisons (and give them the same credit they'd get if they recruited corporations as narcs, only corporations shouldn't be called "sources" because it would carry the stigma of being a narc), the Review approvingly describes the FBI liaison officers working with corporations to promote better Internet hygiene.

> The Review Commission learned that the FBI liaison positions have traditionally been undervalued but that has begun to change as more experienced special agents take on the role, although this has not yet resulted in adequate numbers of assigned special agents or adequate training for those in the position. One field office noted that it had 400 cleared defense contractors (CDCs) in its AOR—ranging from large well known names to far smaller enterprises—with only one liaison officer handling hundreds of CDCs. *This field office emphasized the critical need for more liaison officers to conduct outreach to these companies to promote better internet hygiene*, reduce the number of breaches, and promote long-term cooperation with the FBI.319 Another field office noted, however, some sensitivity in these liaison relationships because labeling private sector contacts as sources could create a stigma. The field office argued that liaison contacts should be considered valuable and special agents should

> receive credit for the quality of liaison relationships the same way they do for CHSs.320

Ed Meese's panel wants the FBI to do the digital equivalent of teaching corporations to blow their nose and wash their hands after peeing, but it doesn't think the FBI should spend time reaching out to Muslim communities but should instead spy on them via paid informants.

Maybe there are good reasons for the panel's disparate recommended treatment of corporations and Muslim communities. If so, the Review doesn't explain it anywhere (though the approach is solidly in line with the Intelligence Committees' rush to give corporations immunity to cyber share information with the federal government).

But it does seem worth noting that this panel has advocated the nanny state for one stakeholder and STASI state for another.

WHAT AN XKEYSCORE FINGERPRINT LOOKS LIKE

As part of its cooperation with New Zealand's best journalist on that country's SIGINT activities, Nicky Hager, the Intercept has published a story on the targets of a particular XKeyscore query (note: these stories say the outlets obtained this document; they don't actually say they obtained it from Edward Snowden): top officials in the Solomon Islands and an anti-corruption activist there.

Aside from the targets, which I'll get to, the story is interesting because it shows in greater detail than we've seen what an XKS query looks

like. It's a fairly standard computer query, though initiated by the word "fingerprint." Some of it is consistent with what Snowden has described fingerprints to include: all the correlated identities that might be associated with a search. The query searches on jremobatu — presumably an email unique name — and James Remobatu, for example. As I have noted, if they wanted to target all the online activities of one particularly person — say, me! — they would add on all the known identifiers, so emptywheel, @emptywheel, Marcy Wheeler, and all the cookies they knew to be associated with me.

What's interesting, though, is this query is not seeking email or other Internet communication per se. It appears to be seeking documents, right out of a file labeled Solomon government documents. Those may have been pulled and stored as attachments on emails. But the query highlights the degree to which XKS sucks up everything, including documents.

Finally, consider the target of the query. As both articles admit, the reason behind some of the surveillance is understandable, if sustained. Australia and New Zealand had peacekeepers in the Solomons to deal with ethnic tensions there, though were withdrawing by January 2013 when the query was done. The query included related keywords.

> In the late 1990s and early 2000s the islands suffered from ethnic violence known as "The Tensions." This led to the 2003 deployment to the Solomons of New Zealand, Australian and Pacific Island police and military peacekeepers. By January 2013, the date of the target list, both New Zealand and Australia were focused on withdrawing their forces from the island country and by the end of that year they were gone.
>
> The XKEYSCORE list shows New Zealand was carrying out surveillance of several terms associated with militant groups on the island, such as "former tension

> militants," and "malaita eagle force." But with the security situation stabilized by 2013, it is unclear why New Zealand spies appear to have continued an expansive surveillance operation across the government, even tailoring XKEYSCORE to intercept information about an anti-corruption campaigner.

More specifically, however, the query was targeting not the militants, but the Truth and Reconciliation process in the wake of the violence.

I would go further than these articles, however, and say I'm not surprised the Five Eyes spied on a Truth and Reconciliation process. I would fully expect NSA's "customer" CIA to ask it to track the South African and Colombian Truth and Reconciliation processes, because the CIA collaborated in the suppression of the opposition in both cases (going so far as providing the intelligence behind Nelson Mandela's arrest in the former case). While I have no reason to expect CIA was involved in the Solomons, I would expect one or more of the myriad intelligence agencies in the Five Eyes country was, particularly given the presence of Aussie and Kiwi peacekeepers there. And they would want to know how their role were being exposed as part of the Truth and Reconciliation process. This query would likely show that.

Which brings me to the point the activist in question, Benjamin Afuga (who sometimes publishes leaked documents) made: this spying, which would definitely detail all cooperation between him and the government, might also reveal his sources.

> Benjamin Afuga, the anti-corruption campaigner, said he was concerned the surveillance may have exposed some of the sources of the leaks he publishes online.

> “I’m an open person – just like an open book,” Afuga said. “I don’t have anything else other than what I’m doing as a whistleblower and someone who exposes corruption. I don’t really understand what they are looking for. I have nothing to hide.”

Ah, but Afuga does have things to hide: his sources. And again, if one or another Five Eyes country had intelligence operatives involved both during the tensions and in the peace keeping process, they would definitely want to know them.

Again, this is all standard spying stuff. I expect CIA (or any other HUMINT agency) would want to know if they’re being talked about and if so by whom – I even expect CIA does a more crude version of this within the US about some of its most sensitive topics, not least because of the way they went after the SSCI Torture investigators.

But this query does provide a sense of just how powerful this spying is in a world when our communications aren’t encrypted.

MINH QUANG PHAM GETS HIS DAY IN SUPREME COURT

I’ve long been tracking the case of Minh Quang Pham, whom I call the “graphic artist of mass destruction” because he is accused of helping Samir Khan on Inspire.

He was detained in the UK back in July 2011 (see the timeline). That December, the UK government tried to strip him of citizenship, but failed because that would have left him

stateless (he's originally from Vietnam but the government doesn't treat him as a citizen). He was quickly charged here when efforts to strip him of UK citizenship failed. But since then, his citizenship case has been wending its way through the British courts.

Throughout this period, it was not officially recognized that Pham was the guy fighting for his citizenship.

Today and yesterday, his case was finally heard before UK's Supreme Court, and his name made public. Here's the Open Society report on his case (which also has a timeline!).

I suppose, if Pham loses, he will be sent to NY for trial. If he wins, he will force the UK to charge him there, which for a variety of reasons may get interesting. Remember: Pham should know the informant behind the UndieBomb 2.0 attack. Which may be why everyone wants to try him over here.

UNDER COVER: THE TARGETS OF STINGS

The NYT brought in Will Arkin (partnering with Eric Lichtblau) to talk about the proliferation of the use of undercover officials in government agencies. The Supreme Court, IRS, the Smithsonian, and DOD are all playing dress up to spy on Americans (and the IRS permits agents to pretend to be lawyers, doctors, clergy, and journalists).

The article makes it clear that — as might be imagined — the drug war is the most common focus of these undercover officers.

> More than half of all the work they described is in pursuit of the illicit drug trade. Money laundering, gangs and

> organized crime investigations make up the second-largest group of operations.

But it doesn't really step back and look at who else is getting targeted, which I've tried to lay on in this stable.

Agency	Target
Supreme Court	Protestors
IRS	Tax evaders
USDA	Food stamp fraud (vendors)
ATF (presumably)	Illegal alcohol and cigarette sales, cigarette smuggling, gun traffickers (Fast & Furious)
Department of Education	Fraud in federally funded ed programs
HHS	Medicare fraudsters
SBA	
NASA	
Smithsonian	
CBP	Drug traffickers
DEA	Drug traffickers
Military investigative agencies	Service members, but increasingly joint work

There are several concerning aspects of this list. I'm hoping the Smithsonian is using under cover officers solely to police the Holocaust and similar museums; the Holocaust museum, after all, has been targeted by a right wing terrorist recently. I might see the point on the Washington Memorial. But I do hope they're no patrolling the Air and Space Museum because they might catch people who, like I did when I was in fifth grade, use the museum as a playground for stupid pre-teen drama while on a field trip.

DOD's expanded use of undercover officers to target Americans is very troubling. The 9th Circuit recently threw out a conviction because the Navy had initiated the case searching data in the guise of protecting Spokane's bases. I suspect, in response, the government will just get more assiduous at laundering such investigations. And it would be highly improper for them to do so clandestinely.

That said, this table is just as telling for what it doesn't include as what it does.

If USDA is going undercover, why not send undercover inspectors to work in food processing

plants, as a great way to not only show the food safety violations, but also the labor violations? Why not go undercover to investigate CAFOs?

The big silence, however, is about bank crime. While I'm sure SEC uses some undercover officers to investigate financial crime, you don't hear of it anymore, since the failed Goldman prosecution. And we know FBI gave up efforts to use undercover officers to investigate (penny ante) mortgage fraud crime because, well, it just forgot.

> 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.

So it's not just that Agencies are using undercover officers to investigate every little thing, including legitimate dissent, with too little oversight.

Its also that the government, as a whole, is using this increasingly to investigate those penny ante crimes, but not the biggest criminals, like the banksters. So long as the choice of these undercover operations reflects inherent bias (and it always has, especially in the war on drugs), then the underlying structure is illegitimate.

JIM COMEY SCOLDS THE PRESS FOR REPORTING ON A COURT FILING

Jim Comey, seemingly intent on squandering once limitless credibility in record time, has written a letter to the NYT to explain two of the FBI's deceptive operations reported recently. The one that's getting the attention — his admission that an agent posed as an AP reporter to catch a teenager making bomb threats — actually comes off as the less indefensible response.

> Relying on an agency behavioral assessment that the anonymous suspect was a narcissist, the online undercover officer portrayed himself as an employee of The Associated Press, and asked if the suspect would be willing to review a draft article about the threats and attacks, to be sure that the anonymous suspect was portrayed fairly.
>
> [snip]
>
> That technique was proper and appropriate under Justice Department and F.B.I. guidelines at the time. Today, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate.

Sure, the FBI decided to dress up as the press to catch someone who hadn't yet done real harm. Sure, they did it to deliver malware, basically a classic hack. Sure, it could have played to this kid's narcissistic tendencies using any number of other fake identities. Sure, this was ultimately going to get made at least as public as a court docket, which does undermine the credibility of a brand name press outlet. But it was a fairly limited operation, that wouldn't

have generated this much attention if Chris Soghoian (in the process of writing a brief to prevent the FBI to hack with even fewer limits) weren't such a meddling hippie.

Having insulted the press by asserting that the FBI playing dress up as the press is legal (though dodging somewhat on whether to do so to catch a teenager would be "proper" today), Comey then responded to the FBI's other recent black eye — being accused of shutting off cable and then pretending to be cable repairmen to access hotel rooms without a warrant — this way.

> The Las Vegas case is still in litigation, so there is little we can say, but it would have been better to wait for the government's response and a court decision before concluding that the F.B.I. engaged in abusive conduct.
>
> Every undercover operation involves "deception," which has long been a critical tool in fighting crime. The F.B.I.'s use of such techniques is subject to close oversight, both internally and by the courts that review our work.

"It would have been better to wait for the government's response and a court decision before concluding that the F.B.I. engaged in abusive conduct"???

Now, the reason the press picked up on this story is because the well-heeled defendants have superb lawyers who wrote a brief that is both engaging and chock full of evidence. The brief starts by laying out the stakes that matter for you and I, even if in this case they affect a bunch of Malaysian men who may have ties to Asian organized crime.

> The next time you call for assistance because the internet service in your home is not working, the "technician" who comes to your door may actually be an undercover government agent. He will

> have secretly disconnected the service, knowing that you will naturally call for help and—when he shows up at your door, impersonating a technician—let him in. He will walk through each room of your home, claiming to diagnose the problem. Actually, he will be videotaping everything (and everyone) inside. He will have no reason to suspect you have broken the law, much less probable cause to obtain a search warrant. But that makes no difference, because by letting him in, you will have "consented" to an intensive search of your home.

Jim Comey thinks the press shouldn't report on this until after the government has had its shot at rebuttal? Does he feel the same about the army of FBI leakers who pre-empt defense cases all the time? Does Comey think it improper for his FBI to have released this press release, upon defendant Wei Seng Phua's arrest, asserting that he is a member of organized crime as a fact and mentioning a prior arrest (not a conviction) that may or may not be deemed admissible to this case?

> According to the criminal complaint, Wei Seng Phua, is known by law enforcement to be a high ranking member of the 14K Triad, an Asian organized crime group. On or about June 18, 2013, Phua was arrested in Macau, along with more than 20 other individuals, for operating an illegal sport book gambling business transacting illegal bets on the World Cup Soccer Tournament. Phua posted bail in Macau and was released.

I didn't see the FBI Director complaining about press stories, written in response to the press release, reported before the defense had been able to present their side.

The point is, one reason we have laws governing open access to court documents — which the

government limits all the time (including with claims about a broad need to hide the methods of its deception) — is so both sides get a bid to make their case, both before judges and before the public. Another reason is so that the press can act as a check on something that may be legal, but probably shouldn't be.

It may well be that FBI gets to use the evidence from their cable repairman scheme (given that superstar appellate lawyer Tom Goldstein is on the case, the defendants probably don't think this is as big of a slam dunk as the press has, probably because Caesars, a competitor with the Asian mob in the gambling industry, was a willing participant in the scheme, including turning *off* the cable service). But that's an entirely different question from whether they should, for precisely the reason the brief lays out: because if the FBI can turn off our cable to set up a cable repairman cover, then it undermines the principle of consensual searches.

These guys may or may not be douchebag Asian mobsters. But they are also being tried in the United States, which still subjects its criminal procedure to fairly broad but by no means unlimited press scrutiny.

Which means the press gets to weigh in. The defense gets to make their case, and if they make a compelling case, the press will report it, just as they almost always report FBI press releases on face value, as they did in this case (to say nothing of FBI's leaks).

Jim Comey, himself a master at working the press, should expect that, and if he wants his FBI to remain credible, should ensure their undercover operations are not just "legal" and "proper" but also "wise."