THE FBI AND CIA UNMINIMIZED COLLECTIONS AND THE HOLES IN ARTICLE III REVIEW OF FISA AMENDMENTS ACT

In my piece confirming that the NSA can search on US person data collected incidentally in Section 702 collection, I pointed to these two paragraphs from the minimization procedures.

> 6(c)
>
> (1) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.
>
> (2) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. FBI will process any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

It’s not clear what this entails.

But Dianne Feinstein once defended the FISA Amendments Act authorization to search on US person information by pointing to Nidal Hasan. Remember, his emails were picked up on a generalized collection of Anwar al-Awlaki’s communications, which should have been a traditional FISA warrant, but may have been conducted via the same software tools as FAA collection. In which case, the kind of access described in the Webster report would provide one idea of what this looks like from the FBI side. That process has almost certainly been streamlined, given that the god-awlful software the FBI used prevented it from pulling the entire stream of Hasan’s emails to Awlaki.

> First, the FBI’s database of intercepts sucked. When the first Hasan intercepts came in, it allowed only keyword searches; tests the Webster team ran showed it would have taken some finesse even to return all the contacts between Hasan and Awlaki consistently. More importantly, it was not until February 2009 that the database provided some way to link related emails, so the Awlaki team in San Diego relied on spreadsheets, notes, or just their memory to link intercepts. (91) But even then, the database only linked formal emails; a number of Hasan’s “emails” to Awlaki were actually web contacts, (100) which would not trigger the database’s automatic linking function. In any case, it appears the Awlaki team never pulled all the emails between Hasan and Awlaki and read them together, which would have made Hasan seem much more worrisome (though when the San Diego agent set the alert for the second email, he searched and found the first one).

Even before this was streamlined, the collection seemed to lack real minimization. Though to be fair, the Agents spending a third of their days

reading Awlaki's emails were drowning and really had an incentive to get reports out as quickly as possible. But they seemed to be in the business of sending out reports with IDs, not the reverse.

In addition, we know that subsequent to that time, the FBI started using this collection (and, I'm quite certain, Samir Khan's), as a tripwire — what they call "Strategic Collections."

> The Hasan attack (and presumably subsequent investigations, as well as the Umar Farouk Abdulmutallab attack) appears to have brought about a change in the way wiretaps like Awlaki's are treated. Now, such wiretaps—deemed Strategic Collections—will have additional follow-up and management oversight.
>
> > The Hasan matter shows that certain [redacted] [intelligence collections] [redacted] serve a dual role, providing intelligence on the target while also serving as a means of identifying otherwise unknown persons with potentially radical or violent intent or susceptibilities. The identification and designation of Strategic Collections [redacted] will allow the FBI to focus additional resources—and, when appropriate, those of [redacted] [other government agencies]—on collections most likely to serve as "trip wires." This will, in turn, increase the scrutiny of information that is most likely to implicate persons in the process of violent radicalization—or, indeed, who have radicalized with violent intent. This will also provide

> > Strategic Collections [redacted] with a significant element of program management, managed review, and quality control that was lacking in the pre-Fort Hood [review of information acquired in the Aulaqi investigation] [redacted].
>
> > If implemented prior to November 5, 2009, this process would have [redacted] [enhanced] the FBI's ability to [redacted] identify potential subjects for "trip wire" and other "standalone" counterterrorism assessments or investigations. (99)

Many many many of the aspirational terrorists the FBI rolled up in 2010 and afterwards were people who had communicated or followed Awlaki or Khan. And to the extent we've prosecuted a bunch of wayward youth who can't pull together a plot without the FBI's assistance, that ought to be a concern on many levels.

Because it would mean this unminimized production is part of the Terror Manufacturing Industry. (Mind you, the FBI was doing this with their own surveillance based off Hal Turner in the 00s, so it's not an approach limited to Muslim radicals.)

To the extent that FAA collection might be sent to FBI as a way to identify non-criminal leads to criminalize, it's a problem, particularly if the FISA Court doesn't see what minimization the FBI uses.

And recall that after the FISA Court of Review opinion forcing Yahoo to comply with Protect America Act collection was unsealed, Russ Feingold made it clear that the companies challenging the Constitutionality of the program didn't have everything they needed to do so. He specifically raised minimization procedures.

> The decision placed the burden of proof on the company to identify problems related to the implementation of the law, information to which the company did not have access. The court upheld the constitutionality of the PAA, as applied, without the benefit of an effective adversarial process. The court concluded that "[t]he record supports the government. Notwithstanding the parade of horribles trotted out by the petitioner, it has presented no evidence of any actual harm, any egregious risk of error, or any broad potential for abuse in the circumstances of the instant case." However, the company did not have access to all relevant information, including problems related to the implementation of the PAA. Senator Feingold, who has repeatedly raised concerns about the implementation of the PAA and its successor, the FISA Amendments Act ("FAA"), in classified communications with the Director of National Intelligence and the Attorney General, has stated that the court's analysis would have been fundamentally altered had the company had access to this information and been able to bring it before the court.
>
> In the absence of specific complaints from the company, the court relied on the good faith of the government. As the court concluded, "[w]ithout something more than a purely speculative set of imaginings, we cannot infer that the purpose of the directives (and, thus, of the surveillance) is other than their stated purpose… The petitioner suggests that, by placing discretion entirely in the hands of the Executive Branch without prior judicial involvement, the procedures cede to that Branch overly broad power that invites abuse. But this is little more than a lament about the risk that government officials will not

> operate in good faith." One example of the court's deference to the government concerns minimization procedures, which require the government to limit the dissemination of information about Americans that it collects in the course of its surveillance. Because the company did not raise concerns about minimization, the court "s[aw] no reason to question the adequacy of the minimization protocol." And yet, the existence of adequate minimization procedures, as applied in this case, was central to the court's constitutional analysis. [bold original, underline mine]

So, at least according to Feingold's description, not only did Yahoo not get the 2007 equivalent of the minimization procedures we now have (which would show holes like the ability to keep purely domestic communications if they posed a threat to corporate property), but they definitely wouldn't get the minimization procedures the FBI and CIA use on secondary distribution of their data (not to mention whatever NCTC gets in tertiary distribution).

In short, Yahoo was blind to all these details, leaving just the government to argue whether that was constitutional or not.

Guess what they argued?

The minimization procedures make it clear just how limited the provider challenges would be.

Then there's this. I have argued since day one that it is meaningless to claim this program is Constitutional if Article III courts have been prevented from reviewing how evidence moves from these programs, through barely minimized distribution at FBI, to an indictment. As the ACLU pointed out yesterday, the government's practice on this front has actually gotten worse since it promised the Supreme Court that defendants charged using this data would be able

to challenge it in court.

> Less than a year ago, the government convinced the Supreme Court to dismiss the ACLU's constitutional challenge to the FISA Amendments Act (FAA)—the controversial warrantless wiretapping statute that is the legal basis for the PRISM program—because our clients couldn't prove that they had been monitored under it. The government repeatedly assured the court that such a restrictive view of who could challenge the law would not forever prevent court review, because criminal defendants who were prosecuted based on evidence obtained under the FAA would be informed of such and would then be able to challenge the statute. Based in part on this assurance, the Supreme Court in February of this year dismissed the case, *Clapper v. Amnesty,* in a 5–4 vote.
>
> But now that the case is closed, we are learning that the government's assurances that it would notify criminal defendants of its reliance on surveillance under the FAA were not what they seemed. Here's one example of the government unequivocally assuring the Supreme Court, in its brief, that criminal defendants would receive notice of FAA surveillance and an opportunity to challenge the statute:
>
> > If the government intends to use or disclose any information obtained or derived from its acquisition of a person's communications under [the FAA] in judicial or administrative proceedings against that person, it must provide advance notice of its intent to the tribunal and the person, whether or not the person was targeted for surveillance under [the FAA].

> In response to questions from the justices at oral argument, the government reiterated this position. Never mind that the government had not notified one criminal defendant about this type of evidence in the five years since the warrantless wiretapping program was written into law.
>
> Ultimately, the Supreme Court accepted the government's position—but, using language almost identical to that in the brief, it highlighted the government's duty to "provide advance notice of its intent" to "use or disclose information obtained or derived" from FAA surveillance.
>
> [snip]
>
> Criminal defendants in Chicago and Florida have filed motions seeking to compel the government to provide notice of its intent to rely on evidence obtained from warrantless wiretapping under the FAA, yet the government is now arguing that it has no obligation to do so. This amounts to a remarkable about-face. These particular defendants have particularly good reason to ask whether evidence against them was obtained under the FAA: In December, Senator Feinstein referenced their cases in testimony urging Congress to reauthorize the FAA's surveillance program. Despite this testimony, the government is fighting the defendants' efforts to understand where the evidence against them has come from, and even told the court that it has no obligation to tell criminal defendants like those in the Florida case whether its evidence came from a *warrantless* interception of communications under the FAA or from more traditional foreign intelligence surveillance.

So the government is giving unminimized data to FBI and CIA, apparently without telling the providers. But when the FBI, at least, uses it, it is increasingly not telling defendants where it came from.

It's not just the Courts that have no scrutiny on all this. Neither do Inspectors General. Last year, Pat Leahy tried (unsuccessfully) to ensure any Inspector General whose department or agency who got to target or minimize data under FAA would be able (though not even required) to review compliance with minimization procedures and report on how many US persons were being swept up in this collection.

> The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community with targeting or minimization procedures approved under this section, with respect to the department or element of such Inspector General—
>
> (A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);
>
> (B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;
>
> (C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent

> possible, whether communications of such targets were reviewed; [my bold emphasizes the new language]

Previously, this was only focused on the Agency that acquired this information – that is, NSA (though DOJ's IG did have access to the data). At the very least, this would expand access to CIA, though probably would expand the scope of DOJ IG's access, not to mention NCTC and anyone else who uses the data.

In short, the minimization procedures (and the unminimized distribution of the data to CIA and FBI, if not also NCTC) create at least three troubling holes in the oversight of the FAA visible:

- Any court challenge before FISC would hide the minimization that is (according to the FISC itself) at the core of any assessment of its constitutionality.
- DOJ and FBI are not – as they promised SCOTUS to do – making it possible to challenge the use of this information via Article III courts.
- Some of the practices of agencies that get this data in bulk, unminimized form escape Inspector General review of those practices.

A lot of NSA apologists complain that those of us who've been reporting on this for years haven't offered any ways to improve this (I have suggested Section 215 be replaced with NSL-based collection). These three holes are obvious ways

to improve the program.

But they’re probably also ways to ensure the program gets Constitutional review. Which may be why the holes, which have been identified repeatedly, never get plugged.