US JUSTICE: A ROTTING TREE OF POISONOUS FRUIT?

Saturday, the NYT reported that other agencies within government struggle to get NSA to share its intelligence with them.

> Agencies working to curb drug trafficking, cyberattacks, money laundering, counterfeiting and even copyright infringement complain that their attempts to exploit the security agency's vast resources have often been turned down because their own investigations are not considered a high enough priority, current and former government officials say.

Of the 1,410 words in the article, 313 words are explicitly attributed to Tim Edgar, who used to work for ACLU but starting in 2006 worked first in the Office of Director of National Intelligence and then in the White House. Another 27 are attributed to "a former senior White House intelligence official," the same description used to introduce Edgar in the article.

The article ends with Edgar expressing relief that NSA succeeded in withholding material (earlier he made a distinction between sharing raw data and intelligence reports) from agencies executing key foreign policy initiatives in the age of cyberwar and Transnational Criminal Organizations, and in so doing avoid a "nightmare scenario."

> As furious as the public criticism of the security agency's programs has been in the two months since Mr. Snowden's disclosures, "it could have been much, much worse, if we had let these other agencies loose and we had real abuses," Mr. Edgar said. "That was the nightmare

> scenario we were worried about, and that hasn't happened."

Today, San Francisco Chronicle reminds that NSA does hand over evidence of serious criminal activities if it finds it while conducting foreign intelligence surveillance, and prosecutors often hide the source of that original intelligence.

> Current and former federal officials say the NSA limits non-terrorism referrals to serious criminal activity inadvertently detected during domestic and foreign surveillance. The NSA referrals apparently have included cases of suspected human trafficking, sexual abuse and overseas bribery by U.S.-based corporations or foreign corporate rivals that violate the Foreign Corrupt Practices Act.
>
> [snip]
>
> "If the intelligence agency uncovers evidence of any crime ranging from sexual abuse to FCPA, they tend to turn that information over to the Department of Justice," Litt told an audience at the Brookings Institution recently. "But the Department of Justice cannot task the intelligence community to do that."
>
> [snip]
>
> "The problem you have is that in many, if not most cases, the NSA doesn't tell DOJ prosecutors where or how they got the information, and won't respond to any discovery requests," said Haddon, the defense attorney. "It's a rare day when you get to find out what the genesis of the ultimate investigation is."
>
> The former Justice Department official agreed: "A defense lawyer can try to follow the bouncing ball to see where

> the tip came from — but a prosecutor is not going to acknowledge that it came from intelligence."

And (as bmaz already noted) Reuters reminds that the DEA has long had its own electronic surveillance capability, and it often hides the source of intelligence as well.

> Although these cases rarely involve national security issues, documents reviewed by Reuters show that law enforcement agents have been directed to conceal how such investigations truly begin — not only from defense lawyers but also sometimes from prosecutors and judges.
>
> The undated documents show that federal agents are trained to "recreate" the investigative trail to effectively cover up where the information originated, a practice that some experts say violates a defendant's Constitutional right to a fair trial. If defendants don't know how an investigation began, they cannot know to ask to review potential sources of exculpatory evidence — information that could reveal entrapment, mistakes or biased witnesses.

As bmaz also noted, none of this was very secret or new. The FISA sharing is clearly permitted by the minimization procedures. Litigation on it 11 years ago suggested it may be even more abusive than laid out under the law. And bmaz has personally been bitching about the DEA stuff as long as I've known him.

These articles suggesting there may be more sharing than the NYT made out on Saturday, then, are primarily reminders that when the fruits of this intelligence get shared, the source of the intelligence often remains hidden from those it is used against.

Which brings me to this WSJ op-ed Edgar

published last week. In some ways the op-ed makes a laudable case for more transparency.

> What, then, accounts for the public mistrust? Intelligence officials forget that the public sees none of this. Where the government sees three branches of government working together in harmony, the public sees a disturbing pattern of secret law and secret government accompanied by demands to "trust us, we are keeping you safe." Secret checks and balances appear to be nothing more than a pale shadow of our constitutional design.
>
> [snip]
>
> President Obama should go further, wresting control from the leakers and restoring trust with the public. He should ask Mr. Clapper to look across the intelligence community and disclose to the public the types of large databases it collects in bulk, under what legal powers or interpretations, and pursuant to what safeguards to protect Americans' privacy—while keeping necessary details secret.
>
> [snip]
>
> Openness is a value in itself, but it is also a necessary precondition to the effective functioning of our three branches of government.

Though it seems to contradict itself as to whether the NSA is collecting everything.

> 'Big data" is one name for the insight that collecting all the information in a massive database will uncover facts that collecting only some of the information cannot. This is not news to Gen. Keith Alexander, director of the National Security Agency. Gen. Alexander is a zealous advocate of getting it all

> whenever practically and legally possible.
>
> [snip]
>
> Despite what Americans see in the movies, the NSA doesn't actually collect everything.

But the truly bizarre part of this op-ed that endorses more transparency is this claim about Amnesty v. Clapper.

> The ACLU has challenged the constitutionality of NSA surveillance programs for years, but that case never got to the issue of constitutional rights. The intelligence community argued, and the Supreme Court agreed, that the civil-liberties groups couldn't maintain their lawsuit. Civil-liberties advocates represented a variety of people with entirely reasonable fears of monitoring. Whether they were actually under surveillance was a secret (**and properly so**). The government argued vigorously that this secrecy meant the case could not go forward, and the court agreed. [my emphasis]

Remember, as a threshold matter, what we're talking about. Amnesty v. Clapper's plaintiffs included human rights organizations like Amnesty International and Human Rights Watch; criminal defense attorneys including Khalid Sheikh Mohammed and Mohamedou Ould Salahi's attorneys by name, the Nation and Chris Hedges, and SEIU.

Since SCOTUS rejected the plaintiffs' case on standing, leaked minimization standards have made it clear Section 702 surveillance provides no protection for human rights workers, journalists, political organizations, or even attorneys representing people — like Salahi — who have not yet been criminally charged. While none of the plaintiffs in the case could be directly targeted, their communications with

people they have every business to be talking to easily could be. And we'd never know whether these entities — whose work makes them adversaries to the government — were surveilled unless the government decided to charge them or their interlocutors and reveal that fact.

And Tim Edgar, civil libertarian, thinks it is "proper" that all these people, most of whose activities are protected under the Constitution, should never know if the government is surveilling their work.

Then there's the other problem with Edgar's endorsement of secrecy surrounding whether Amnesty v. Clapper plaintiffs have been surveilled: the government has reneged on the several promises it made over the course of that litigation to reveal when this surveillance is used on defendants (precisely the issue the SFChron and Reuters stories emphasize).

> What we have learned since the *Clapper* decision, however, has revealed a yawning chasm between the government's words and actions. Faced with recent revelations_about the FAA surveillance program, intelligence officials have raced to defend the controversial law. And, in doing so, they have touted at least four cases where warrantless FAA surveillance was purportedly critical to preempting terrorist plots. Yet not one of the defendants in these prosecutions was told that the government's evidence was obtained from FAA surveillance, and thus they had no opportunity to challenge the statute. This fact runs directly contrary to the arguments that lawyers for the government paraded before the Supreme Court just last fall.
>
> Indeed, the government has openly departed from its previous position. 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 extends to the program Edgar specifically defends in his op-ed, the Section 215 dragnet, where the government never told Basaaly Saaed Moalin it used the Section 215 dragnet — apparently accessed by claiming al-Shabaab's pre-terrorist designation effort to expel US-backed invaders of Somalia amounted to plotting against "the homeland" — to identify and justify wiretaps on him.

Given Edgar's enthusiasm for the surveillance of even protected activities to remain secret, taken in tandem with all the known examples where the government hides the source of this surveillance, there is no reason to believe an article based significantly on his claims that NSA's information (whether in raw data form or as intelligence reports) is not shared widely in the government. Maybe it's true.

But ultimately we have one way of testing such claims: in the courts. And if even defendants are never given an opportunity to challenge not just the constitutionality of the programs themselves, but also potentially dubious claims made to justify the surveillance, all the so-called transparency from those already caught in lies is of limited use.