# THE NYPD'S SURVEILLANCE OF MUSLIMS AND OCCUPY WALL STREET CONVERGES

I started my morning reading with this AP Q&A on the significance of their series on the NYPD's spying on Muslims. There are several things missing: why does the NYPD profile only businesses they believe to be owned by Muslims, and not the American chains at which recent immigrants also congregate? Why doesn't the Q&A discuss how the NYPD-on-the-Hudson got close to, but missed the two most significant plots of recent years; what does that say about the efficacy of all this spying? And why doesn't the Q&A discuss the many informants the NYPD has deployed?

That said, the AP does get to the core reason why the NYPD's program abuses the First Amendment:

> Bloomberg and his aides have not addressed, however, why police kept intelligence files on innocuous mosque sermons and plans for peaceful protests. They've not explained why police noted which restaurants served "devout" Muslims, why police maintained lists of Muslims who changed their names or why innocent people attending Friday prayer services were photographed and videotaped.
>
> Those activities, many Muslims said, make them feel like they're under scrutiny just because of their religion.

After reading that Q&A, I then read this NYT article, talking about how the NYPD's intelligence division—the CIA-on-the-Hudson

again—has preemptively arrested some Occupy Wall Street protestors before they engaged in protest.

> On Nov. 17, Kira Moyer-Sims was near the Manhattan Bridge, buying coffee while three friends waited nearby in a car. More than a dozen blocks away, protesters gathered for an Occupy Wall Street "day of action," which organizers had described as an attempt to block the streets around the New York Stock Exchange.
>
> Then, Ms. Moyer-Sims said, about 30 police officers surrounded her and the people in the car.
>
> All four were arrested, said Vik Pawar, a lawyer for Ms. Moyer-Sims and two of the others, and taken to a police facility in the East Village. He said officers strip-searched them and ignored their requests for a lawyer.

These are the same tactics—or worse—as used when the NYPD targeted Muslims planning a peaceful protest of cartoons deemed blasphemous. But most troubling is the last anecdote the NYT reports (which the NYT might have known to contextualize if they had been reporting on the NYPD spying on Muslims). In one case, they NYPD **and the FBI** are targeting an Occupy activist who, as someone who appears to have changed his name from his birth name, would have been targeted closely under the NYPD program. And they appear to be insinuating a tie with Islamic terrorism.

> Mark Adams, a 32-year-old engineer from Virginia, said he was arrested in November at an Occupy Wall Street protest in Midtown and was questioned by a police detective and an agent from the Federal Bureau of Investigation, who asked about his involvement with Occupy Wall Street, **requested his e-mail address** and **inquired whether he had ever**

> **been to Yemen or met anyone connected to Al Qaeda**.
>
> Mr. Adams, a naturalized United States citizen who was **born in Pakistan**, said he was arrested during another protest in January and questioned by intelligence division detectives. In that instance, he said, the detectives asked him about specific names and addresses, asked about his work history, education and family, and **questioned him about a trip he had made to Ireland**.
>
> Mr. Adams said he was disturbed that anyone would consider him a threat because of his ethnicity or political views. “It’s scary,” he said. [my emphasis]

As the AP reported last October, the NYPD conducts extensive checks and keeps records on those within the city who change their names from Arabic or Muslim-sounding names to something Americanized.

> The NYPD monitors everyone in the city who changes his or her name, according to internal police documents and interviews. For those whose names sound Arabic or might be from Muslim countries, police run comprehensive background checks that include reviewing travel records, criminal histories, business licenses and immigration documents. All this is recorded in police databases for supervisors, who review the names and select a handful of people for police to visit.
>
> [snip]
>
> David Cohen, the NYPD’s intelligence chief, worried that would-be terrorists could use their new names to lie low in New York, current and former officials recalled. Reviewing name changes was intended to identify people who either

> Americanized their names or took Arabic names for the first time, said the officials, who insisted on anonymity because they were not authorized to discuss the program.
>
> NYPD spokesman Paul Browne did not respond to messages left over two days asking about the legal justification for the program and whether it had identified any terrorists.
>
> The goal was to find a way to spot terrorists like Daood Gilani and Carlos Bledsoe before they attacked.

I assume Mark Adams is not the name Adams was given when he was born in Pakistan. And so because he apparently did something that David Headley also did—change his name from his Pakistani birth name to something more Anglo—he appears to have come under scrutiny for potential terrorist ties. Because he changed his name, it appears, he got asked whether he ever went to Yemen and what he was doing on a trip to Ireland.

I've been predicting this since the moment NYPD Counterterrroism officer Tony Bologna pepper sprayed innocent women.

But the NYPD-FBI treatment of Mark Adams is troubling for another reason. Note they asked for his email address. Given the absurdly low standards under the PATRIOT Act, which requires only that information be "relevant to" a terrorism investigation, the FBI would presumably be able to get Adams' email contacts and financial information using National Security Letters and get other information (such as geolocation under the secret PATRIOT program) using Section 215 of the PATRIOT Act.

In other words, the NYPD, apparently using their theories about name changes as a potential marker for terrorism, have found their nexus that opens up a whole set of tools under the PATRIOT Act.

# FIRST THEY CAME FOR RUSS FEINGOLD, THEN THEY CAME FOR CATO

As I've followed all the really interesting commentary on the Koch Brothers' efforts to take over Cato (Dave Weigel, Jonathan Adler, Jane Mayer, Brad DeLong) I keep thinking back to this Adam Serwer post last year, pointing out one of the most anti-libertarian moves they made: dumping $25,000 to beat the biggest defender of civil liberties in the Senate.

> Another way to put this is that the Kochs will happily put their money behind candidates who agree with their economic agenda but disagree with their social agenda. They will never put their money behind candidates of whom the reverse is true.

The best example of this I can think of is the Senate's lost liberaltarian **Russ Feingold**. Feingold was the only senator to vote against the PATRIOT Act. He was one of the first senators to endorse marriage equality. He voted against the war in Iraq, against TARP and financial reform, and has consistently sought to rein in the surveillance state. He was, however, also one of the architects of campaign-finance reform along with **John McCain** and a supporter of the health-care bill and the stimulus.

When Feingold's candidacy was in danger, the Koch's poured their money into the coffers of Feingold's opponent, **Ron Johnson**. According to the FEC, the Koch brothers each gave him individual

> contributions of $2,400, while KochPAC gave him $10,000. Charles Koch's son **Chase Koch** gave Johnson $5,800, while David's* wife **Julia Koch** gave another $2,400. An **Elizabeth Koch** from the same zip code in Wichita as Charles and Julia gave an additional $2,400. All in all, the Koch family gave Johnson more than $25,000 to send Russ Feingold home. What type of candidate were they supporting?
>
> Johnson is anti-marriage equality, anti-choice, has no problem with open-ended military engagements and he supports the PATRIOT Act with some caveats, but only because "you have **Barack Obama** in power versus **George Bush**. I wasn't overly concerned with George Bush in power."
>
> [snip]
>
> In other words, faced with one candidate who shares their views on social issues and national security and another who shares their views on economic issues, the Kochs chose the latter.

Libertarianism, which was fostered to offer ideological cover for laissez faire capitalism, is now being actively replaced by its biggest patrons with a TeaParty ideology that has been co-opted over the last three years to offer populist cover for unrestrained capitalism.

So while I am fascinated by Corey Robin's critique of Julian Sanchez' presignation,

> When the Kochs wield their money at Cato, that's hegemony. But when they do it in Wisconsin, that's democracy.

I think Robin's comments on this year's Ron Paul debate among the left is far more important.

> Our problem—and again by "our" I mean a left that's social democratic (or welfare state liberal or economically progressive or whatever the hell you

> want to call it) and anti-imperial—is that we don't really have a vigorous national spokesperson for the issues of war and peace, an end to empire, a challenge to Israel, and so forth, that Paul has in fact been articulating. The source of Paul's positions on these issues are not the same as ours (again more reason not to give him our support). But he is talking about these issues, often in surprisingly blunt and challenging terms. Would that we had someone on our side who could make the case against an American empire, or American supremacy, in such a pungent way.
>
> This, it's clear, is why people like Glenn Greenwald say that Paul's voice needs to be heard. Not, Greenwald makes clear, because he supports Paul, but because it is a terrible comment—a shanda for the left—that we don't have anyone on our side of comparable visibility launching an attack on American imperialism and warfare. (Recalling what I said in the context of the death of Christopher Hitchens, I suspect this has something to do with our normalization and acceptance of war as a way of life.) In other words, we need to listen to Paul, not because he's worthy of our support, and certainly not because the reasons that underlie his positions on foreign policy are ours, but because he reveals what's not being said, or not being said enough, on our side.
>
> [snip]
>
> Ron Paul is unacceptable, and it's unacceptable that we don't have someone on the left who is raising the issues of imperialism, war and peace, and civil liberties in as visible and forceful a way.

Russ Feingold is gone from the Senate. As of last night, Dennis Kucinich will be gone from the House next year. For what it's worth, Ron Paul, too, will be gone from the House. In my own neighborhood, we hope Justin Amash, who hopes to assume Paul's mantle, is gone from the House too.

There are other voices stepping up. But even Ron Wyden, who is a lonely voice criticizing the Obama Administration's most egregious civil liberties abuses, offered somewhat tempered criticism of Attorney General Holder's speech on Monday.

> Attorney General Holder's speech today is a welcome step in the right direction, but further steps need to be taken, and they need to be taken soon.

The government—both Republican and Democratic—has spent billions to create a climate of fear. It has succeeded in leading people to accept the assault on civil liberties without even questioning efficacy, much less constitutionality or abuse.

Meanwhile, even more money is being dumped into a reframed ideology of unrestrained capitalism, one with a populist face unembarrassed by its own inconsistency.

So I'll go even further than Alex Pareene, who lists all the reasons we should care about the Koch takeover attempt on Cato. There is a case to be made for the Constitution and for executive restraint. We on the left need to get more effective at making it. Because the capitalist case is in the process of being bought out.

# HOW GOOD ARE DOJ'S REASONS FOR BURYING ITS CASE AGAINST ANWAR AL-AWLAKI?

Today's the day Eric Holder explains how his Department decided it was okay to kill a US citizen with no independent legal review, even while he says we should use civilian courts to, uh, give terrorists due process.

Now, at least as of late January, the Administration still planned not to include any real information about its case against Anwar al-Awlaki in Holder's speech.

> As currently written, the speech makes no overt mention of the Awlaki operation, and reveals none of the intelligence the administration relied on in carrying out his killing.

Since much of the evidence that has been used to implicate Awlaki came from Umar Farouk Abdulmutallab, I'm going to return to a question I first raised several weeks ago, why DOJ sat on the information it got from Abdulmutallab implicating Awlaki so long.

In this post, I considered why DOJ published a narrative explicitly describing Anwar al-Awlaki's role in Umar Farouk Abdulmutallab's terror plot last month, rather than when it learned the information from Abdulmutallab sometime in 2010. The reason is likely evidentiary. It appears the government never persuaded Abdulmutallab to testify against Awlaki even while he was implicating Awlaki during "plea negotiations," meaning it's unclear Abdulmutallab would have repeated the information implicating Awlaki in court. Note, since that post, Abdulmutallab prosecutor Jonathan Tukel confirmed in court that the UndieBomber was offered—but did not accept—a

plea agreement.

In this post, I will consider other reasons why DOJ may have buried (and presumably will continue to bury) their case against Awlaki: a desire to hide its signals intelligence, its informants, as well as a desire to win legal cases.

**Wiretaps on Awlaki had already been exposed**

I've laid out a timeline of select events and disclosures below. But I want to start from this article, published the day after Abdulmutallab fired his public defenders in 2010, presumably putting an end to hopes to get him to testify against Awlaki publicly. It noted that charging Awlaki would require the US to rely on wiretaps and confidential informants.

> Charging al-Awlaki with having direct involvement in terrorism could require the U.S. to reveal evidence gleaned from foreign wiretaps or confidential informants.

The issues with the terms of Abdulmutallab's "plea negotiations" aside, was that a credible reason to hide the intelligence on Awlaki?

With respect to the wiretaps, no.

Crazy Pete Hoekstra made it clear in November 2009—over a month before Awlaki was first targeted by a US drone—that NSA had been wiretapping him for at least a year. In reporting in the days after Abdulmutallab's attack, anonymous sources made it clear the NSA had (belatedly) discovered intercepts discussing the plot, too.

> Other intelligence linking al-Awlaki to Abdulmutallab only became apparent after the attempted bombing, including communications intercepted by the National Security Agency that indicated that the cleric was meeting with "a Nigerian" in preparation for some kind of operation, according to a U.S.

> intelligence official.

The intelligence revealed last month—detailing how Awlaki tested Abdulmutallab's interest in jihad before they met—doesn't seem to compromise NSA's wiretaps any more than Hoekstra already did.

> Defendant provided this individual with the number for his Yemeni cellular telephone. Thereafter, defendant received a text message from Awlaki telling defendant to call him, which defendant did. During their brief telephone conversation, it was agreed that defendant would send Awlaki a written message explaining why he wanted to become involved in jihad. Defendant took several days to write his message to Awlaki, telling him of his desire to become involved in jihad, and seeking Awlaki's guidance. After receiving defendant's message, Awlaki sent defendant a response, telling him that Awlaki would find a way for defendant to become involved in jihad.

It seems the government could have released this information months earlier, and certainly should never have been declared a state secret.

That said, the intercept information doesn't make the case that Awlaki ordered Abdulmutallab to strike the US. So even if the government had released that information, it wouldn't have justified targeting Awlaki with a drone.

**The need to protect confidential informants**

I'm much more sympathetic to DOJ's concerns about revealing details obtained from confidential informants—because there is good reason to believe we had at least a few double agents working within AQAP, at least two of whom went through Saudi Arabia's "deradicalization" program.

As the timeline below shows, before Abdulmutallab showed up in Yemen, former Gitmo detainee Mazin Salih Musaid al-Awfi, who had "rejoined" al Qaeda in Yemen, returned from Yemen to Saudi Arabia, a possible double agent. Then, at about the same time Abdulmutallab was headed to Yemen, AQAP bombmaker Ibrahim al-Asiri's brother, Abdullah, tried to assassinate then Saudi Interior Minister Mohammed bin Nayef. Asiri used Nayef's willingness to work with "repentant jihadis" to get close to him. As such, the plot may have been an attempt to retaliate against Nayef for his efforts at "deradicalization." Most famously, Jabir al-Fayfi, who worked with AQAP for two years, returned to Saudi Arabia in October 2010; Fayfi would have been with AQAP when Abdulmutallab was training with the group and would have been able to provide information on him—and Awlaki (I understand that Fayfi implicated others far more than he did Awlaki, though, so in a sense, that would have hurt DOJ's case against Awlaki).

The threat to suspected informants is real and ongoing; a few weeks ago, the rebranded AQAP group Ansar al-Sharia executed three men suspected of providing targeting intelligence to the US.

Note, though, intelligence on Abdulmutallab's training shouldn't have been that hard to collect. In his superb story on Yemen, Jeremy Scahill reported that a tribal leader he traveled with and discussed on the record had met the UndieBomber, as well as top AQAP leaders. One would hope that what Scahill can get in a several week trip, our intelligence operatives can learn in lengthier deployments.

It's not really clear whether and how much of what the government released last month came from alternative intelligence sources. My guess is that information on Abdulmutallab's training, such as the detail that he met Samir Khan and unnamed others, came from or at least was supplemented by others. And given that the government doesn't name the person who

introduced Abdulmutallab to Awlaki—the narrative explains, "defendant made contact with an individual who in turn made Awlaki aware of defendant's desire to meet him"—I suspect they may have learned this detail from someone else.

That leaves the big question: was someone like Fayfi close enough to Awlaki in December 2009 to corroborate the key detail that Awlaki ordered Abdulmutallab?

If so, by that point Yemen had already made it clear that Fayfi was one source of the intelligence on the toner cartridge plot.

The example of Fayfi also reveals non-safety reasons why the government might not want to release the intelligence it has on Awlaki. First, Fayfi implicated others more than Awlaki, so his testimony might have exonerated Awlaki. In addition, tying intelligence about Awlaki directly to Fayfi would raise questions about whether we've used Gitmo to persuade people to spy for us—not to mention, the accuracy of such information, particularly since a number of detainees were known to fabricate information to please Gitmo handlers. By the time Fayfi returned to Saudi Arabia, OLC had already authorized the killing of Awlaki; what would we have done if Fayfi refuted the intelligence we used to target Awlaki?

So while a desire to hide informants is a more reasonable excuse for hiding the information on Awlaki than a desire to hide the wiretapping that Hoestra exposed in 2009, not all of the reasons the government would want to do so are laudable.

**The government wouldn't say because it didn't want to lose a lawsuit**

The other reason the government may have withheld information—which is utterly absurd but nevertheless a possible explanation—is that it didn't want to lose any lawsuits over the information.

That, at least, was the reason Kathryn Ruemmler

opposed the speech Holder will give today last November.

> Another senior official expressing caution about the plan was Kathryn Ruemmler, the White House counsel. She cautioned that the disclosures could weaken the government's stance in pending litigation. *The New York Times* has filed a lawsuit against the Obama administration under the Freedom of Information Act seeking the release of the Justice Department legal opinion in the Awlaki case.

But if that's what motivates Obama's lawyer, then it has been an issue throughout the time the Administration has refused to release its case against Awlaki. For example, Scott Shane must have FOIAed for the OLC memo on Awlaki's killing within days of its completion (we don't know what date in June 2010 OLC finalized the memo, but Shane FOIAed the memo on June 11, 2010). The next month, Awlaki's father retained ACLU and Center for Constitutional Rights to sue to prevent the son's killing except if he were an imminent threat. That suit was submitted on August 30, 2010, and not dismissed until December 7 of that year. And in the immediate aftermath of the Awlaki killing on September 30 of last year, Charlie Savage submitted a new FOIA for the memo, and Public Record Media and the ACLU followed suit later the same year. At least the NYT and ACLU are suing to force disclosure of the memo.

In other words, since just two months after the last interrogations of Abdulmutallab provided to Dr. Simon Perry—but several months before he fired his lawyers, presumably ending any hope that a plea deal would lead to Abdulmutallab's testimony against Awlaki—the government has been in at least one legal proceeding regarding the legal justification for killing Awlaki. It still is. And the White House Counsel thinks that's a good reason to prevent any more from coming out.

All of these reasons provide yet another reason to institute some kind of due process. Using CIPA, the government could submit much of this intelligence in a means that can be made public.

But instead, we're left with one court filing—the Abdulmutallab one—summarizing things Abdulmutallab refused to say in a trial and … still more rumors.

**Timeline**

February 18, 2009: Possible double agent Mazin Salih Musaid al-Awfi leaves AQAP

August 2009: Abdulmutallab travels to Yemen to seek Awlaki

August 2009: Abdullah al-Asiri attempts to assassinate Mohammed bin Nayef by posing as repentant jihadi

November 9, 2009: Pete Hoekstra reveals government has been intercepting Awlaki's communications going back at least a year

December 25, 2009: Abdulmutallab confesses that an Abu Tarak ordered him to strike the US

December 26, 2009 to January 28, 2010: Abdulmutallab refuses to talk

January 19, 2010: US designates AQAP terrorist group

January 29, 2010 to February 23, 2010: The main period of Abdulmutallab's interrogations

By April 6, 2010: Awlaki placed on CIA's kill list

April 8, 16, 30, 2010: Abdulmutallab interrogated 3 more times and asked about Awlaki's death

June 2010: OLC authorizes Awlaki's killing

June 11, 2010: Scott Shane FOIAs OLC memo on Awlaki killing

July 2010: Nasser al-Awlaki retains ACLU/CCR to sue for due process

July 16, 2010: US declares Awlaki a designated terrorist

August 30, 2010: ACLU, CCR sue to limit killing of Awlaki to imminent threat

September 8-9, 2010: Jabir al-Fayfi rounded up by Yemen.

September 13, 2010: Abdulmutallab fires his lawyers, citing a conflict of interest

September 14, 2010: DOJ considers charges against Awlaki but worries about relying on information from wiretaps or confidential informants

September 25, 2010: Government opposes ACLU/CCR suit to force government to show due process, in part by invoking state secrets

October 29, 2010: Toner cartridge plot exposed by presumed double agent Jabir al-Fayfi

December 7, 2010: Judge John Bates dismisses ACLU/CCR Awlaki suit

August 28, 2011: Government commits not to use Abdulmutallab's confessions implicating Awlaki directly at trial

September 23, 2011: Government requests protective order for item apparently pertaining to Awlaki and Abdulmutallab

September 30, 2011: Anwar al-Awlaki killed in drone strike

October 7, 2011: Charlie Savage FOIAs OLC memo

October 11, 2011: Opening arguments in Abdulmutallab trial

October 12, 2011: Abdulmutallab pleads guilty

October 19, 2011: ACLU FOIAs Anwar al-Awlaki OLC memo, underlying evidence supporting it, and information relating to Samir Khan and Abdullah al-Awalaki

November 2011: Administration decides to partially release information pertaining to

Awlaki's death

February 10, 2012: Government releases narrative implicating Awlaki

---

# ACCORDING TO DOD INSPECTOR GENERAL DEFINITION, BRADLEY MANNING DID NOT "LEAK"

The unclassified version of the DOD Inspector General report on leaks within DOD over the last three years (that is, during the Obama Administration) defines "leak" this way.

> Unauthorized disclosure of SCI [Secure Compartmented Information] to the public which is defined as: "A communication or physical transfer of [SCI]information to an unauthorized recipient." DoDD 5210.50, Section 3.2, "Unauthorized Disclosure of Classified Information to the Public," dated July 22, 2005. [second bracket original]

A leak is a leak of Secure Compartmented Information, not just classified information.

To be sure, the report's own insertion of that second bracket makes it clear this definition applies to this report. Congress focused on SCI information when it ordered the IG to do the report in a classified annex of this fiscal year's Defense Appropriation:

> The investigation shall contain the following: an inventory of the leaks of SCI data including those attributed to a "senior administration official" from

> the past three calendar years; the actions taken to investigation each of the events; which of the investigations were referred to the Department of Justice; and what additional actions were taken after the Department of Justice investigation.

The House Appropriations Committee didn't require the IG to inventory all classified leaks, just the SCI ones.

Nevertheless, as defined, Bradley Manning's alleged leaks are classified, not SCI.

Whereas this report shows that people from Obama's Administration, including at least one senior administration official, have been leaking SCI.

> We confirmed with DoD components that some unauthorized disclosures of SCI to the public did occur within DoD between December 23, 2008 and December 23, 2011. Among the unauthorized SCI disclosures to the public reported, a DoD Senior Official was directly attributed as a source of unauthorized SCI disclosures to the public. DoD components also reported that they followed established DoD guidance and procedures for forwarding unauthorized disclosure cases to the Department of Justice for action when appropriate.

Now, again, this report is the unclassified version; I'm sure the report provided more detail in the classified version sent to the Chair and Ranking Member of 10 different committees and subcommittees.

But note what this results paragraph doesn't say. While it confirms at least one of the leaks from a senior administration official was unauthorized, it only cataloged the **unauthorized** leaks, suggesting there may be more SCI leaks that were authorized (consider, for example, the

leaks of a range of compartment names to Bob Woodward, which John Rizzo suggested were part of “one big authorized disclosure,” or reported cooperation between DOD and CIA and Hollywood on the movie about Osama bin Laden’s killing, itself the subject of a different investigation).

Further, while Congress mandated the IG do so, this unclassified report does not explain what happened to these SCI leak referrals at DOJ. Has DOJ been pursuing the SCI leaks by senior administration officials as diligently as it has pursued people like Thomas Drake, who was charged with *retaining* information, much of it of disputed classification?

One thing’s clear: whether to make political hay or out of genuine concern about the Administration leaks, Congress is honing in on how many of these leaks were authorized and whether DOJ investigated the unauthorized ones. Granted, the most interesting results here remain classified (let’s see whether the 10 committees and subcommittees can withstand the temptation of leaking a classified report on leaking).

But it does begin to show that the Administration that has accused more leakers of “espionage” than all others combined itself leaks far more sensitive information.

(h/t Steven Aftergood who first reported on the IG Report)

---

# DJIBOUTI’S CABLE NEWS

Remember back in 2008, when a mysterious cluster of intercontinental cables were cut, knocking parts of the Middle East and South Asia (notably Egypt and Pakistan) off telecom networks?

Well, we’ve got another cluster of cut cables

again, this time off of Djibouti, where one of our currently most critical bases is (we operate into Yemen and Somalia from there).

> Undersea data cables linking East Africa to the Middle East and Europe were severed in two separate shipping accidents this month, causing telecommunications outages in at least nine countries and affecting millions of Internet and phone users, telecom executives and government officials said.
>
> A ship dragging its anchor off the coast of the Kenyan port city of Mombasa severed a crucial Internet and phone link for the region Saturday, crippling electronic communications from Zimbabwe to Djibouti, according to a public-private consortium that owns the undersea cable.
>
> The Indian Ocean fiber-optic cable, known as The East African Marine Systems, or Teams, is owned by a group of telecom companies and the Kenyan government. It was the fourth cable to be severed in the region since Feb. 17.
>
> The Teams cable had been rerouting data from three other cables severed 10 days ago in the Red Sea between Djibouti and the Middle East. Together, the four fiber-optic cables channel thousands of gigabytes of information per second and form the backbone of East Africa's telecom infrastructure.

There are, undoubtedly, a number of interesting conversations that would be transiting those telecom lines, not least those between AQAP and al-Shabaab. Not to mention the conversations within East Africa.

But those conversations won't be traveling by most easily accessible telecommunication channels, at least not until those cables are

restored.

And while we're discussing Internet cables, note that these Djibouti cables, like those off of Egypt that were taken out in 2008, do not appear on State's cable—classified just Secret—of critical infrastructure around the globe.

---

# JEH JOHNSON ON THE "MILITARY'S DOMESTIC LEGAL AUTHORITY"

In addition to suggesting that the 16 year old American citizen Abdulrahman al-Awlaki was a legitimate military target, Jeh Johnson spoke yesterday about the "military's domestic legal authority." Now, rest assured, Johnson said the Administration does not rely on aggressive interpretations of such authority.

> Against an unconventional enemy that observes no borders and does not play by the rules, we must guard against aggressive interpretations of our authorities that will discredit our efforts, provoke controversy and invite challenge.

He acknowledges that posse comitatus requires express authorization from Congress before extending the reach of the military onto US soil.

> As I told the Heritage Foundation last October, over-reaching with military power can result in national security setbacks, not gains. Particularly **when we attempt to extend the reach of the military on to U.S. soil**, the courts resist, consistent with our core values

> and our American heritage — reflected, no less, in places such as the Declaration of Independence, the Federalist Papers, the Third Amendment, and in the 1878 federal criminal statute, still on the books today, which prohibits willfully using the military as a posse comitatus **unless expressly authorized by Congress or the Constitution**. [my emphasis]

Then he proceeds directly from describing the express authorization required from Congress to a discussion of the AUMF—**as the basis for the "military's domestic legal authority."**

> Second: in the conflict against al Qaeda and associated forces, **the bedrock of the military's domestic legal authority continues to be the Authorization for the Use of Military Force** passed by the Congress one week after 9/11.[2] "The AUMF," as it is often called, is Congress' authorization to the President to:
>
> > use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.
>
> Ten years later, the AUMF remains on the books, and it is still a viable authorization today. [my emphasis]

Then Johnson describes how the Administration—with no express authority from Congress until the NDAA—stretched an

authorization limited to those people and groups with ties to 9/11 to include those "associated with" such groups. And, again with no express authorization from Congress, expanded it to include those who "engaged in hostilities" with coalition partners.

> In the detention context, we in the Obama Administration have interpreted this authority to include:
>
> > those persons who were part of, or substantially supported, Taliban or al-Qaeda forces or associated forces that are engaged in hostilities against the United States or its coalition partners.[3]
>
> This interpretation of our statutory authority has been adopted by the courts in the habeas cases brought by Guantanamo detainees,[4] and in 2011 Congress joined the Executive and Judicial branches of government in embracing this interpretation when it codified it almost word-for-word in Section 1021 of this year's National Defense Authorization Act, 10 years after enactment of the original AUMF.[5] (A point worth noting here: contrary to some reports, neither Section 1021 nor any other detainee-related provision in this year's Defense Authorization Act creates or expands upon the authority for the military to detain a U.S. citizen.)

Johnson doesn't mention, of course, that the government is using the same interpretation to extend the military's domestic legal authority to non-detention areas. Those applications are secret, you see.

Note, in this passage, how Johnson gracefully re-specifies that he's talking about the 2001 AUMF, and not the 2002 AUMF, which also remains in effect?

> But, the AUMF, the statutory authorization from 2001, is not open-ended.  It does not authorize military force against anyone the Executive labels a "terrorist."  Rather, it encompasses only those groups or people with a link to the terrorist attacks on 9/11, or associated forces.

That's important because the government at least used to—and presumably still does (otherwise they wouldn't have panicked when Congress considered repealing the AUMF authorizing a war that is supposed to be over)—rely on the Iraq AUMF to target "anyone the Executive labels a 'terrorist.'"

Given that the Iraq AUMF has been used to go beyond the definitions in the 2001 AUMF, I'll skip the paragraphs were Johnson talks about how narrow the government's interpretation of "associated forces" is.

Particularly because this paragraph is my very favorite bit in this entirely disingenuous speech.

> Third: there is nothing in the wording of the 2001 AUMF or its legislative history that restricts this statutory authority to the "hot" battlefields of Afghanistan.  Afghanistan was plainly the focus when the authorization was enacted in September 2001, but the AUMF authorized the use of necessary and appropriate force against the organizations and persons connected to the September 11th attacks – al Qaeda and the Taliban – without a geographic limitation.

Pretty comprehensive, huh, Jeh? Neither the wording of the AUMF or the legislative history limits the AUMF, right?

That of course leaves out what Tom Daschle has said explicitly.

> Just before the Senate acted on this compromise [AUMF] resolution, the White House sought one last change. Literally minutes before the Senate cast its vote, the administration sought to add the words "in the United States and" after "appropriate force" in the agreed-upon text. This last-minute change would have given the president broad authority to exercise expansive powers not just overseas – where we all understood he wanted authority to act – but right here in the United States, potentially against American citizens. I could see no justification for Congress to accede to this extraordinary request for additional authority. I refused.

Jeh Johnson, you see, admits that the military needs express authority from Congress to operate within the US. Congress expressly refused to grant that authority. Johnson knows that, surely. Nevertheless, there he was yesterday, laying out the "military's domestic legal authority" that Congress never expressly authorized.

Remember, "domestic legal authority," he's talking about, not—or not just—international legal authority. Which is why this passage is so funny.

> The legal point is important because, in fact, over the last 10 years al Qaeda has not only become more decentralized, it has also, for the most part, migrated away from Afghanistan to other places where it can find safe haven.
>
> However, this legal conclusion too has its limits.  It should not be interpreted to mean that we believe we are in any "Global War on Terror," **or that we can use military force whenever we want, wherever we want. International legal principles, including respect for a state's**

> **sovereignty** and the laws of war, impose important limits on our ability to act unilaterally, and on the way in which we can use force in foreign territories. [my emphasis]

In the context of talking about the military's domestic legal authority, Jeh Johnson says that state sovereignty will protect us. Not the Tenth Amendment, mind you, but the sovereign right of **other** states to keep the US out.

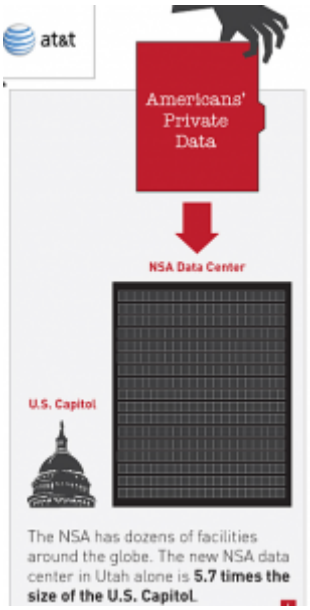
But who will keep the US out of the US?

I guess Johnson was relying on the kids at Yale Law being credulous when he said the Administration "guard[s] against aggressive interpretations of our authorities"?

---

# WILL SCOTUS INVENT A "DATABASE-AND-MINING" EXCEPTION TO THE FOURTH AMENDMENT?

As I noted yesterday, the Administration appealed the 2nd Circuit Decision granting review of the FISA Amendments Act to the Supreme Court last week. I wanted to talk about their argument in more detail here.




Over at Lawfare, Steve Vladeck noted that this case would likely decide whether and what the "foreign intelligence surveillance" exception to the Fourth Amendment, akin to "special needs" exceptions like border searches and drug testing.

> ***Third***, if the Court affirms (or denies certiorari), this case could very well finally settle the question whether the Fourth Amendment's Warrant Clause includes a "foreign intelligence surveillance exception," as the FISA Court of Review held in the *In re Directives* decision in 2008. That's because on the merits, 50 U.S.C. § 1881a(b)(5) mandates that the authorized surveillance "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." Thus, although it is hard to see how surveillance under § 1881a could violate the Fourth Amendment, explication of the (as yet unclear) Fourth Amendment principles that govern in such cases would necessarily circumscribe the government's authority under this provision going forward (especially if *In re Directives* is not followed…).

I would go further and say that this case will determine whether there is what I'll call a database-and-mining exception allowing the government to collect domestic data to which no reasonable suspicion attaches, store it, data mine it, and based on the results of that data mining use the data itself to establish cause for further surveillance. Thus, it will have an impact not just for this warrantless wiretapping application, but also for things like Secret PATRIOT, in which the government is collecting US person geolocation data in an effort to be able to pinpoint the locations of alleged terrorists, not to mention the more general databases collecting things like who buys hydrogen peroxide.

I make a distinction between foreign intelligence surveillance and "database-and-mining" exceptions because the government is, in fact, conducting domestic surveillance under these programs and using it to collect intelligence on US persons (indeed, when asked about Secret PATRIOT earlier this month, James Clapper invoked "foreign or domestic" intelligence in the context of Secret PATRIOT). The government has managed to hide that fact thus far by blatantly misleading the FISA Court of Review in *In re Directives* and doing so (to a lesser degree) here.

In *In re Directives*, the government misled the court in two ways. First, according to Russ Feingold, the government didn't reveal (and the company challenging the order didn't have access to) information about how the targeting is used. The amendments he tried to pass—and which Mike McConnell and Michael Mukasey issued veto threats in response to—suggest some of the problems Feingold foresaw and the intelligence community refused to fix: reverse targeting, inclusion of US person data in larger data mining samples, and the retention and use of improperly collected information.

The government even more blatantly misled the FISCR with regards to what it did with US person

data.

> The petitioner's concern with incidental collections is overblown. It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions to not render those acquisitions unlawful.9 [citations omitted] The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.
>
> 9 The petitioner has not charged that the Executive Branch is surveilling overseas persons in order intentionally to surveil persons in the United States. Because the issue is not before us, we do not pass on the legitimacy vel non of such a practice.

The notion that the government doesn't have this US person data in a database is farcical at this point, as the graphic above showing the relative size of the NSA's data center in UT—which I snipped from this larger ACLU graphic—makes clear (though the government's unwillingness to be legally bound to segregate US person data made that clear, as well). As I suggested when this decision was released, the government must have been offering non-denial denials of having such a collection of US person data back in 2007.

> Did the court ask only about a database consisting entirely of incidentally collected information? Did they ask whether the government keeps incidentally collected information in its existing databases (that is, it doesn't have a database devoted solely

> to incidental data, but neither does it pull the incidental data out of its existing database)? Or, as bmaz reminds me below but that I originally omitted, is the government having one or more contractors maintain such a database? Or is the government, rather, using an expansive definition of targeting, suggesting that anyone who buys falafels from the same place that suspected terrorist does then, in turn, becomes targeted?

As I showed yesterday, the government is already doing something similar with this suit, simply ignoring the part of the suit pertaining to the completely legal retention of purely domestic communications, so long as it was ostensibly collected unintentionally.

Their larger argument, too, does something similar, using a definition of "targeting" that tautologically excludes US persons in principle but not in fact.

> Section 1881a does not authorize surveillance targeting respondents or any other United States person, 50 U.S.C. 1881a(b)(1)-(3), and respondents have presented no evidence that their international communications have ever been incidentally acquired by the government in its surveillance of non-United States persons abroad.

Of course, it takes two to communicate, so for every single targeted conversation, there is a counterparty whose communications are also collected. Nevertheless, the government focuses on authorizations—the word "targeting"—to distract from these counterparties. Note too, here, how once again the government ignores 1881a(b)(4), which permits the retention of incidentally collected domestic communications.

One of the real tells, though, comes in what

appears to be a throwaway intended to prove there are people who would have standing to sue under FAA.

> If the government intends to use or disclose any information obtained or derived from its acquisition of a person's communications under Section 1881A in judicial or administrative proceedings against that person, it must provide advance notice of its intent to the tribunal and the person, even if the person was not targeted for surveillance under Section 1881A. 50 U.S.C. 1881e(a); see 50 U.S.C. 1801(k), 1806(c).

The government's reference to the possibility it would use data "even if the person was not targeted for surveillance" admits that it does collect and review the communications of those not targeted, potentially even for law enforcement purposes. But then it suggests that the only way people could be aggrieved is if their communications were used for law enforcement, not intelligence.

Yet the plaintiffs argument for injury is that they cannot do their jobs—NGOs, lawyers, reporters—even if their communications become subject to intelligence, not law enforcement, collection. Their question, of course, is whether domestic intelligence collected under the guise of foreign intelligence constitutes a violation of the Fourth Amendment, whether the government has a database-and-mining exception under the Fourth Amendment.

That may not change SCOTUS' analysis on standing. But it does make it clear that—no matter how the government would like to distract from this point—US person data (even entirely domestic conversations) can be legally collected and analyzed under this law.

So that is what the stakes are. The government would love to have SCOTUS either deny cert or affirm the district finding that the plaintiffs

don’t have standing, particularly before Jewel, which addresses the underlying issue of dragnet collection. The government would also love to use such a SCOTUS action, in secret, to rule that its use of GPS tracking in the intelligence, which it is busy distinguishing from a law enforcement context under *Jones*, context is legal. The government would also like any challenge to pertain to a specific order (as it would be under 1881e), so it can hide what it does with the data it collects once it goes into the database in UT.

And given what Russ Feingold said back in 2008—that an adversary process would reveal both the potential for abuse, and quite possibly the abuse, the government really really doesn’t want this case to move forward.

---

# BILL KELLER BLAMES LEAK ARRESTS THAT PRECEDED WIKILEAKS ON WIKILEAKS

Bill Keller has another narcissistic column attacking Julian Assange. The whole thing is rubbish not worth your time, but I did want to unpack the complaint with which Keller ends his column.

> “A lot of attention has been focused on WikiLeaks and its colorful proprietors,” Aftergood told me. “But the real action, it turns out, is not at the publisher level; it’s at the source level. And there aren’t a lot of sources as prolific or as reckless as Bradley Manning allegedly was.”
>
> For good reason. The Obama administration has been much more

> aggressive than its predecessors in pursuing and punishing leakers. The latest case, the arrest last month of John Kiriakou, a former C.I.A. terrorist-hunter accused of telling journalists the names of colleagues who participated in the waterboarding of Qaeda suspects, is symptomatic of the crackdown. It is this administration's sixth criminal case against an official for confiding to the media, more than all previous presidents combined. The message is chilling for those entrusted with keeping legitimate secrets and for whistleblowers or officials who want the public to understand how our national security is or is not protected.
>
> Here's the paradox the documentaries have overlooked so far: **The most palpable legacy of the WikiLeaks campaign for transparency is that the U.S. government is more secretive than ever**. [my emphasis]

The Obama Administration has charged 6 people with some kind of espionage charge for leaking:

- Thomas Drake was indicted on April 10, 2010, just days after the release of the Collateral Murder video and before Bradley Manning first contacted Adrian Lamo; he was charged for purported leaks going back to February 2006
- Shamai Leibowitz was first investigated in mid-2009, before Manning leaked anything to WikiLeaks; he was charged on December 4, 2009 and sentenced on May

24, 2010, the day the government was first learning about Lamo's conversations with Manning

- Stephen Jin-Woo Kim was indicted on August 19, 2010, around the time DOD first started trying to figure out what Manning allegedly sent to WikiLeaks; he is alleged to have leaked in June 2009
- Manning was arrested on May 29, 2010 and will be formally charged this week for leaks allegedly starting in November 2009
- Jeffrey Sterling was indicted on December 22, 2010, around the time the government was trying to pressure Manning into testifying about Assange; his leaks allegedly started in 2001
- John Kiriakou was charged on January 23, 2012 for leaks dating back to 2007

All the non-WikiLeaks leaks allegedly took place before Manning's. All were formally charged before Manning, and all but two men were arrested before Manning.

And yet Bill Keller, in a demonstration of his typical reporting skill though not Newtonian physics, suggests that WikiLeaks caused the crackdown on leaks.

WikiLeaks **can't** be the reason the government has cracked down so harshly, because most of the

crackdown preceded the key WikiLeaks publications.

Perhaps Keller is just looking for some easy explanation for why Kiriakou got busted. As I have shown, the most logical way to establish the case against Kiriakou (short of the now legal acquisition of journalist call records using NSLs) was through the NYT article reporting Deuce Martinez' role in interrogating Khalid Sheikh Mohammed. And while Kiriakou's recklessness—as a CIA guy who leaked a covert officer's identity through apparently unencrypted email—rivals Manning's, security expert Chris Soghoian has pointed out how shoddy (and far inferior to WikiLeaks') the NYT's own security is.

The government is prosecuting leaks at a degree unheard of—and has been since before WikiLeaks. It is using new interpretations that strip journalists of the privacy expectations they once had. But along with that, journalists have taken a while to adjust to the new intrusiveness.

The government deserves most of the blame for it. But the NYT seems to deserve more of the blame for shoddy security than WikiLeaks does.

---

# THE GOVERNMENT DOESN'T WANT TO TALK ABOUT COLLECTING DOMESTIC COMMUNICATIONS UNDER FAA


On Friday, the government appealed the 2nd Circuit's decision that Amnesty International and other NGOs and individuals have standing to challenge the FISA Amendments Act. I'll have a post on the implications of their substantive argument shortly. But in the meantime, I wanted to note what they're not even addressing.

The image to the left is a fragment of the government's references to statutes and regulation mentioned in its brief; it's the part of the list referring to the part of the FAA in question. As you can see, it almost—but not quite—lists every clause of the law.

One clause notably missing from the almost-sequential list above is 1881a(b)(4), which reads,

> [An acquisition authorized under subsection (a)] may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

And while it mentions clauses that refer back to this restriction (for example, 1881a(c)(1), 1881a(d), 1881a(g)(2)(A)(i), etc), it never goes back and includes this language—the requirement that the government not intentionally acquire communications that are located entirely within the US—in its argument. (There are other clauses the brief ignores, a number of which pertain to oversight of the certifications the government has made; I may return to these at a future

time.)

Or, to put it another way, the government never admits that **the FAA permits the purportedly unintentional collection of entirely domestic communication**.

And yet that is a part of this lawsuit. The original complaint in this suit invoked this clause:

> An acquisition under section 702(a) may not … "intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States
>
> [snip]
>
> Moreover, the Attorney General and the DNI may acquire purely domestic communications as long as there is uncertainly about the location of one party to the communications.

And the 2nd Circuit opinion (authored by Gerard Lynch) referenced this clause:

> "Targeting procedures" are procedures designed to ensure that an authorized acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and is designed to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."
>
> [snip]
>
> In addition, the certification must attest that the surveillance complies with statutory limitations providing that it:
>
> [snip]

> (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;
>
> [snip]
>
> Under the FAA, in contrast to the preexisting FISA scheme, the FISC may not monitor compliance with the targeting and minimization procedures on an ongoing basis. Instead, that duty falls to the AG and DNI, who must submit their assessments to the FISC, as well as the congressional intelligence committees and the Senate and House Judiciary Committees.
>
> [snip]
>
> But the government has not asserted, and the statute does not clearly state, that the FISC may rely on these assessments to revoke earlier surveillance authorizations.

Now, to some degree, the government might argue it ignored the clause prohibiting intentional—but not accidental—targeting of domestic communications because the plaintiffs' primary basis for establishing standing is their frequent communication with likely targets overseas. As I'll show, the government wants to make this case about a particular definition of a target, and key to that argument is a claim that it is impossible for the plaintiffs to be targets.

Yet therein lies one of the key problems with their argument, given that 1881a(b)(4) only prohibits the plaintiffs from being intentional targets; the FAA very pointedly did not prohibit the government from keeping US person information it "unintentionally" collected. In fact, Mike McConnell and Michael Mukasey started issuing veto threats when Russ Feingold tried to restrict the ongoing use of domestic

communications identified as such after the fact.

Finally, in the one case that approved this kind of collection (though under the Protect America Act, not the FAA) used targeting procedures to substitute for particularity required under the Fourth Amendment. Under PAA, those procedures were not mapped out by law; under FAA they are, partly in the clause the government wants to ignore.

And yet, remarkably, the government doesn't want that clause to be part of its discussion with SCOTUS. Seeing as how even the FISA Court of Review finds that substitute for particularity—the targeting procedures—to be a key part of compliance with the Fourth Amendment, you'd think that would be relevant.

---

# DOJ'S UNTRACKED EMAIL SPYING

As Wired reports, DOJ blew off the requirement that it tell Congress how many pen registers and trap and trace devices they used for the entire Bush Administration.

> […]the Justice Department was not following the law and had not provided Congress with the material at least for years 2004 to 2008. On the flip side, Congress was not exercising its watchdog role, thus enabling the Justice Department to skirt any oversight whatsoever on an increasingly used surveillance method that does not require court warrants, according to Justice Department documents obtained via the Freedom of Information Act.

But just as interesting as DOJ's failure to

follow the law on disclosing these surveillance tools are two details from the emails Chris Soghoian liberated to make all this clear.

First, note the December 23, 2009 email from Janet Webb (on PDF 4) revealing that DOJ's agencies weren't tracking email pen registers (that is, lists of who was emailing each other), and one of them—they speculate DEA—still wasn't in 2009.

> FBI only began keeping computer intercept stats a couple of years ago. The other agency may be DEA.

From which we might assume DEA is engaging in a ton of email tracking they don't want to tell anyone about?

Wired suggests why they may not be tracking such information.

> Another feature of [the Electronic Communication Privacy Act] had once protected Americans' electronic communications from the government's prying eyes, but it has become so woefully outdated that it now grants the authorities nearly carte blanche powers to obtain Americans' e-mail stored in the cloud, such as in Gmail or Hotmail — without a court warrant.

That is, we probably should assume these email numbers are so small—and DEA isn't tracking them at all—because they're just taking them, with no court oversight at all.

The other detail to remember about these reports is they include only criminal surveillance, not intelligence surveillance. Russ Feingold staffer Lara Flint makes that clear in her request, and DOJ staffer Mark Agrast makes it clear in his response. They're getting that information via other means, presumably NSLs or Section 215.

So while they're hiding a lot of the cloud computer spying they're doing in the name of

criminal investigations, that doesn’t even scratch the surface of the degree to which they’re tracking who emails whom.