ON SOLIDARITY IN THE FACE OF MUSLIM REGISTRY PLANS

People have made well-meaning promises to sign up to any Muslim registry. But given the logic of current lists targeting Muslims, that will be hard to do.

IMAGINE IF APPLE WERE A POWERLESS MUSLIM?

In a piece on the Apple case, Amy Davidson tried to imagine the unintended consequences of broadening the application of the All Writs Act in this case.

> If a case involving a non-digital phone network could be applied to smartphones, what technologies might an Apple precedent be applied to, three or four decades from now? (The N.S.A. used, or rather promiscuously misused, another pen-register case from the same era to justify its bulk data collection.) It no longer becomes fanciful to wonder about what the F.B.I. might, for example, ask coders adept in whatever genetic-editing language emerges from the recent developments in CRISPR technology to do. But some of the alarming potential applications are low-tech, too. What if the government was trying to get information not out of a phone but out of a community? Could it require someone with distinct cultural or linguistic knowledge not only to give it information but to use that expertise to devise ways for it to infiltrate that

> community? Could an imam, for example, be asked not only to tell what he knows but to manufacture an informant?
>
> This is the situation that Apple is in, and that all sorts of other companies and individuals could be in eventually. There are problems enough with the insistence on a back door for devices that will be sold not only in America but in countries with governments that feel less constrained by privacy concerns than ours does. And there are reasons to be cynical about technology companies that abuse private information in their own way, or that jump in to protect not a principle but their brands. But the legal precedent that may be set here matters. By using All Writs, the government is attempting to circumvent the constitutionally serious character of the many questions about encryption and privacy. It is demanding, in effect, that the courts build a back door to the back-door debate.

She raises fair points.

Except when I read them, I thought instead of the demands FBI has already made.

FBI demanded that Lavabit turn over a key protecting all of its users to try to get to Edward Snowden, which led Ladar Levison to shut down the business, well before it got to the point where Ted Olson (who's now helping Apple make its case, and presumably will all the way to the Supreme Court) would help him argue a legal case.

More directly on point to Davidson's scenarios, there are numerous reports of FBI creating some artificial means of coercion — often having to do with immigration — that effectively force speech of a certain kind. That's not far off Davidson's example of an Imam being forced to inform (which, especially given the use of

Section 215 to collect data to identify informants, might involve coercion of a different kind).

Obviously, Apple is huge and rich and powerful so it has the ability to fight such coercion (or just leave the country).

But the comparison is especially apt, I think, because it speaks to why the FBI might be willing to make such breath-taking demands from Apple. It's used to demanding coercion, whether from smaller ISPs or Imams or Muslim immigrants. And because those people have no power to fight back, FBI has grown used to such ability to coerce cooperation.

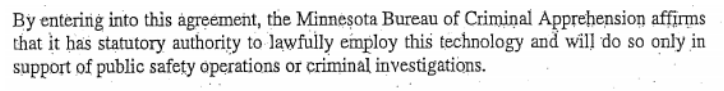
STINGRAYS AND PUBLIC SAFETY OPERATIONS

In my piece on the loopholes in the new Stingray policy, I noted that public safety applications for Stingray use might fall under what the policy calls the "exceptional circumstances" that aren't exigent but nevertheless don't require a warrant.

> I'm not sure whether the exigent/emergency use incorporates the public safety applications mentioned in the non-disclosure agreements localities sign with the FBI, or if that's included in this oblique passage.
>
> > There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. In such cases, which we expect to

> > be very limited, agents must first obtain approval from executive-level personnel at the agency's headquarters and the relevant U.S. Attorney, and then from a Criminal Division DAAG. The Criminal Division shall keep track of the number of times the use of a cell-site simulator is approved under this subsection, as well as the circumstances underlying each such use.
>
> In short, many, if not most, known uses are included in exceptions to the new policy.

We know there *are* public safety applications, because they are permitted even to localities by FBI's Non-Disclosure Agreements.


By entering into this agreement, the Minnesota Bureau of Criminal Apprehension affirms that it has statutory authority to lawfully employ this technology and will do so only in support of public safety operations or criminal investigations.

I suspect these uses are for public events to both track the presence of known targets and to collect who was present in case of any terrorist event or other serious disruption. Indeed, for a lot of reasons — notably the odd testimony of FBI's telecom forensics witness, the way FBI's witnesses were bracketed off from investigators, and some oddness about when and how they found the brothers' phones (and therefore the brothers) — I suspect someone was running Stingrays at the Boston Marathon. A Stingray (or many) deployed at public events to help protect them (assuming, of course, the terrorists that attack such an event aren't narcs for the DEA, as people have speculated Tamerlan Tsarnaev was).

Newsweek asked DOJ whether that exceptional circumstances paragraph covered the use of Stingrays in public places included in a policy released by the FBI in December and they confirmed it is (here's my post on the December

release, which anticipates all the loopholes in the policy I IDed the other day).

> In December 2014, the FBI, which falls under Justice Department's new policy, explained to members of Congress the situations in which it does not need a warrant to deploy the technology. They include: "(1) cases that pose an imminent danger to public safety, (2) cases that involve a fugitive, or (3) cases in which the technology is used in public places or other locations at which the FBI deems there is no reasonable expectation of privacy."
>
> *Newsweek* reached out to the Justice Department to determine whether its new policy allows the FBI to continue using stingrays without warrants in public places. In short, it does, fitting within the policy's "exceptional circumstances" category.
>
> "If somebody is in a public park, that is a public space," Patrick Rodenbush, a Justice Department spokesman, says as an example, adding the condition that "circumstances on the ground make obtaining a warrant impracticable," though he did not elaborate on what "impracticable" entails. But the dragnet nature of stingray collection means cellphone data of a person sitting in a nearby house may be picked up as well. "That's why we have the deletion policy that we do," Rodenbush responds. "In some cases it's everyday that [bystander information] is deleted, it depends what they are using it for.… In some cases it is a maximum of 30 days."
>
> He adds: "The circumstances under which this exception will be granted will be very limited. Agents operating under this exception are still required to obtain a court order pursuant to the Pen Register Statute, and comply with the

> policy's requirements to obtain senior-level department approval."

Equally important as admitting that DOJ will use this in public places (like big sporting events) is Rodenbush's confirmation that DOJ will obtain *only* Pen Registers for these uses.

That means they'll virtually never get noticed to defendants, because the government will claim the evidence did not get introduced in court (just as no evidence collected from a Stingray was introduced, if they were used, in Dzhokhar's case; in Dzhokhar's case there was always another GPS device that showed his location).

The more I review this new policy and the December one the more I'm convinced they change almost nothing except the notice to the judge and the minimization (both still important improvements), except insofar as they recreate ignorance of Stingray use precisely in cases like public safety operations.

IN 2015, CIA WILL PROACTIVELY RESPOND TO THE "DIGITAL REVOLUTION"

I noted some weeks ago about how John Brennan — who had failed spectacularly on cybersecurity while at the White House but then learned the joys of hacking targets when he spied on the Senate Intelligence Committee — was rolling out a cyber directorate.

On Wednesday and yesterday, Brennan rolled out that change amid a larger restructuring.

In a troubling sign, the plan twice refers to the "digital revolution" as if it were in progress right now, not something that has already happened and is now our status quo. "Second, we must be positioned to embrace and leverage the digital revolution to the benefit of all mission areas." But don't worry, because Brennan says this reorganization will prevent the CIA from suffering the fate of Kodak, which didn't anticipate digital cameras. CIA is embracing the "digital revolution" so it doesn't miss the next one, I guess, as it did with the Arab Spring.

With all the focus on the digital directorate, however, I think there are aspects of this reorganization plan that are far more worthy of note.

First, the whole thing reads like a mid-1990s business reorganization plan, organized into "themes" and speaking of "investing in our people" and a new Talent Development Center of Excellence and embracing and modernizing and blah blah blah. That's troubling, because those jargon-driven reorganizations usually failed after some Mitt Romney type had stripped the entity in question for cash. At least in the unclassified description of the reorganization, the plan seems better served to attract credulous investors than to effect change.

Just as telling, the unclassified plan says nothing about how CIA will retain what linguistic and cultural skills it has after it shifts to a more topical and less geographic structure. Digital analysis is nice, but there will come a time when someone is going to have read the content that metadata has identified, and we can't simply rely on foreign partners to do this or we'll be susceptible to their disinformation.

Finally, there's this section:

> ***Theme Three: Modernize the way we do business.*** The pace of world events and technological change demands that Agency

leaders be able to make decisions with agility, at the appropriate level, with the right information, and in the interests of the broader enterprise. We must have the capacity to make the sound strategic decisions needed to build a better Agency and run it efficiently, even as we respond to urgent external requirements. We must empower our officers to address the operational, analytical, technological, support, and other issues that are at the heart of what we do every day. Accordingly, we will:

- ***Enhance and empower the Executive Director's role and responsibilities to manage day-to-day organizational functions, including overseeing a revamped corporate governance model.***
- ***Create a restructured Executive Secretary office*** *to streamline core executive support functions, thereby increasing effectiveness and efficiency.*
- *Even as we improve our ability to govern and make decisions and streamline our processes at the enterprise level, there*

> *will be a corresponding effort to delegate decisionmaking and accountability for achieving mission to the lowest appropriate level and to streamline our processes and practices throughout the Agency.*

Perhaps I should just trust Brennan here, because he has served as both Chief of Staff to the Director and Deputy Executive Director, so he knows how these critical management roles function. But it also sounds like a bid to have the Director's immediate staff more involved in the nitty gritty of operations, perhaps akin to the way the White House National Security Council (where Brennan has served more recently) has done the same with operations, in part to bypass oversight. If Brennan wants to make it easier to hold officers accountable for fuck-ups, great. But if Brennan wants to make it easier to conduct ill-considered operations without a grown-up objecting, it'll lead to more problems from the CIA.

Alfreda Bikowsky has been the model of the analyst-who-sticks-her-nose into the operations function that seems to be the goal here. The CIA thinks she's great, but she's also the poster child for hackishness, abuse, and in some cases obstinate stupidity. I wish Brennan the best of luck in making CIA a more effective agency. I just hope he doesn't end up making it still more problematic.

WHY ARE THE US MARSHALS AT THE CENTER OF ALL THESE PEN REGISTERS?

The US Marshal Service shows up prominently in two Pen Register stories from yesterday.

First, as part of a great story from WSJ's Jen Valentino-Devries mapping out how many federal criminal electronic records requests never get unsealed…

> In eight years as a federal magistrate judge in Texas, Brian Owsley approved scores of government requests for electronic surveillance in connection with criminal investigations—then sealed them at the government's request. The secrecy nagged at him.
>
> So before he left the bench last year, the judge decided to unseal more than 100 of his own orders, along with the government's legal justification for the surveillance. The investigations, he says, involved ordinary crimes such as bank robbery and drug trafficking, not "state secrets." Most had long since ended.
>
> A senior judge halted the effort with a one-paragraph order that offered no explanation for the decision and that itself was sealed.

She released this summary of all the Federal Pen Register/Trap and Trace requests in 2012. As she pointed out on Twitter, the greatest number of requests don't come from FBI. They come from the USMS, which submitted almost half of all requests that year, with 9,132.

Then, the ACLU revealed that, just before an appointment to view Sarasota, Florida's requests

under the Pen Register authority to use Stingray IMSI catchers to identify cell locations, the US Marshals declared control over the records, claiming they had deputized the local cop who had made the requests.

> Over the past several months, the ACLU has filed dozens of public records requests with Florida law enforcement agencies seeking information about their use of controversial cell phone tracking devices known as "stingrays." (The devices are also known as "cell site simulators" or "IMSI catchers.") Stingrays track phones by mimicking service providers' cell towers and sending out powerful signals that trick nearby phones — including phones of countless bystanders — into sending their locations and identifying information.
>
> The Florida agencies' responses to our requests have varied widely, with somestonewalling and others releasing records. The most recent request went to the Sarasota Police Department, and the fallout from that request has raised red flag after red flag.
>
> **RED FLAG #1:** The Sarasota Police initially told us that they had responsive records, including applications filed by and orders issued to a local detective under the state"trap and trace" statute that he had relied on for authorization to conduct stingray surveillance. That raised the first red flag, since trap and trace orders are typically used to gather limited information about the phone numbers of incoming calls, not to track cell phones inside private spaces or conduct dragnet surveillance. And, such orders require a very low legal standard. As one federal magistrate judge has held, police should be

> permitted to use stingrays only after obtaining a probable cause warrant, if at all.
>
> **RED FLAG #2:** The Sarasota Police set up an appointment for us to inspect the applications and orders, as required by Florida law. But a few hours before that appointment, an assistant city attorney sent an email cancelling the meeting on the basis that the U.S. Marshals Service was claiming the records as their own and instructing the local cops not to release them. Their explanation: the Marshals Service had deputized the local officer, and therefore the records were actually the property of the federal government.
>
> [snip]
>
> **RED FLAG #3:** Realizing we weren't going to get hold of the Sarasota Police Department's copies of the applications and orders anytime soon, we asked the county court if we could obtain copies from its files. Incredibly, the court said it had no copies. The court doesn't even have docket entries indicating that applications were filed or orders issued. Apparently, the local detective came to court with a single paper copy of the application and proposed order, and then walked out with the same papers once signed by a judge.
>
> Court rules — and the First Amendment — require judges to retain copies of judicial records and to make them available to the public, but the court (and the detective) completely flouted those requirements here.

Valentino-Devries notes that a lot of the records being kept secret also involve cell location.

> In 2011, magistrate judges in California complained that investigators were applying for pen registers without explicitly saying they wanted to use sophisticated cellphone-location trackers, called “stingrays,” which can be used to locate suspects. Stingrays gather phone-number information, along with other data transmitted by cellphones, by acting as fake cellphone towers. The 1986 surveillance law doesn’t contemplate such technology.
>
> Mr. Owsley, the former Texas magistrate judge, says he had similar concerns about applications for “cell-tower dumps,” in which agents can obtain records of all phones within range of specified cell towers over time—including people who aren’t suspected of a crime.

While we don’t yet know how many of the 9,000 requests the Marshals made in 2012 were for location data, the coincidence is mighty interesting.

The Marshals do have cause to search for suspects’ location. They claim they arrest over 300 wanted fugitives a day. That’s where stingrays would be particularly useful, as they would help to identify the location of a known suspect.

So how often are the Marshals using stingrays to do their work? And to what degree do they do so hiding behind even more obscure local pen register laws to do so?

ACLU TO JIM COMEY:

WELCOME. NOW FIX THIS.

Jim Comey has officially been in charge of the FBI for less than two weeks.

Today, in honor of Constitution Day, the ACLU just released a report showing how the FBI's expanded mandate since 9/11 has led to Constitutional abuses.

Most of the details of the report have been reported here in depth. But the Big Data section includes some details I haven't covered. It explains:

FBI collects Suspicious Activities Reports that duplicate — but lower the standard for — an existing database

> Another major problem is that eGuardian effectively competes with another federal government SAR. The Intelligence Reform and Terrorism Prevention Act of 2004 established the Information Sharing Environment (ISE) to serve as the conduit for terrorism-related information sharing between state and local law enforcement and the federal government.114 A March 2013 Government Accountability Office report found that though the two programs share information between them, eGuardian uses a lower evidentiary threshold for inclusion of SARs, which creates risks and privacy problems.
>
> The Government Accountability Office found that "many fusion centers have decided not to automatically share all of their ISE-SARs with eGuardian" because eGuardian doesn't meet ISE standards.115 One fusion center said it would never provide SARs to eGuardian because of the fusion center's privacy policy.116 The Government Accountability Office also found that the two systems

> "have overlapping goals and offer duplicative services."117

FBI will soon have the equivalent of 20 pieces of intelligence on every American — and they share this broadly

> An FBI budget request for fiscal year 2008 said the FBI had amassed databases containing 1.5 billion records, and two members of Congress described documents predicting the FBI would have 6 billion records by 2012, which they said would represent "20 separate 'records' for each man, woman and child in the United States."119
>
> [snip]
>
> According to a 2012 Systems of Records Notice covering all FBI data warehouses, the information in these systems can be shared broadly, even with foreign entities and private companies, and for a multitude of law enforcement and non-law enforcement purposes.133

There's far more in the report, chronicling the slow creep of abusive FBI techniques since 9/11.

Sadly, given that this has all been treated as legal, I doubt that Comey will do anything about it, even with ACLU's demonstration that the dragnet has led FBI to miss real crimes.

REAL ~~ID~~ BIOMETRICS IN IMMIGRATION BILL

I've got two ginormous issues with the report that the Immigration Bill includes a measure that would require the creation of a "photo tool" database to verify status before

employment.

> The immigration reform measure the Senate began debating yesterday would create a national biometric database of virtually every adult in the U.S., in what privacy groups fear could be the first step to a ubiquitous national identification system.
>
> Buried in the more than 800 pages of the bipartisan legislation (.pdf) is language mandating the creation of the innocuously-named "photo tool," a massive federal database administered by the Department of Homeland Security and containing names, ages, Social Security numbers and photographs of everyone in the country with a driver's license or other state-issued photo ID.
>
> Employers would be obliged to look up every new hire in the database to verify that they match their photo.

First, this would accomplish precisely what Real ID would accomplish, but less.

I've long believed we were going to go to Real ID in any case. I've also long believed that we ought to change the politics of such a discussion by proposing that along with Real ID, we also get universal registration. The authoritarians would thus have a choice: give up their efforts to disenfranchise the poor via voter ID and track employment, or lose both.

I'm guessing it'd present quite a dilemma for the authoritarians.

But to learn a bipartisan bill is basically ceding on real ID without using it to foster democracy?

My other problem has to do with the certainty that this would be turned into a counterterrorism tool. Recall that last year, John Brennan decided protecting US person data was just too tough, so National Counterterrorism

Center would have to have access to any federal database that NCTC deemed to have terrorism information.

I think it highly likely that NCTC would deem a database of all Americans to contain terrorist information.

Therefore, we should assume that whatever else this database is supposed to do, it would also mean that the faces of innocent Americans would start getting included in the data analysis of potential terrorists.

Mind you, the authorities claim (though I'm not convinced) that they weren't able to ID the Tsarnaev brothers with all the images they had of them at the Boston Marathon. Maybe the technology sucks (again, not convinced).

But that doesn't stop the inclusion of all Americans in the dataset of possible terrorist mugshots from being an invitation for witch hunts.

FACEBOOK A BETTER SPOOK THAN RAY KELLY

We have been discussing the FBI's apparent inability to use the multiple images of the Tsarnaev brothers from the Boston Marathon to ID them using facial recognition software.

So I wanted to circle back to two things. First, point to the passage of BoGlo's comprehensive account of the hunt for the brothers that pertains to this question.

Of note, it says photo analysts had isolated the video of Dzhokhar dropping his backpack by Wednesday morning.

> When Alben, of the State Police, saw the results of the analysts' work on

> Wednesday morning, he couldn't believe it: they had captured an image of the young man in a white hat dropping a backpack outside the Forum restaurant and then walking away.
>
> "There was a eureka moment . . . It was right there for you to see," said the colonel. "It was quite clear to me we had a breakthrough in the case."
>
> They had faces. Now they needed names.

The account remains unclear about why the FBI was unable to match the images, relying on speculation about the quality of the images.

> Even after authorities isolated the images of the two suspected bombers, they weren't able to pinpoint the suspects' identities — an essential puzzle piece that was still missing Wednesday.
>
> The FBI has poured millions of dollars into facial recognition technology over the years so it can quickly cross-check an image against millions of other pictures in government databases.
>
> In this case, both brothers were already in existing government databases, including the Massachusetts Registry of Motor Vehicles and federal immigration records. They were legal immigrants from the former Soviet republic of Kyrgyzstan, in theory allowing the FBI to find their names.
>
> But it's not clear which databases the FBI checked. And it may not have mattered. The pictures, taken from surveillance cameras above street level, were likely far too grainy when zoomed in on the brothers' faces. And the older brother was wearing sunglasses, making their task even harder.
>
> In addition, unlike in a traditional mug

> shot, the camera wasn't looking at their faces head-on.
>
> Investigators worked feverishly Wednesday trying to identify the men, searching other photos and video, trying to find high-definition images.
>
> "We still needed more clarity," said Alben, of the State Police. "As good as the videos were, we needed more clarity."

And in the middle of this account, BoGlo suggests that briefing Deval Patrick about being able to ID the face of the suspect led directly to the mistaken press reports — based on solid sources, the outlets insisted at the time — that authorities were ready to arrest a suspect.

> Colonel Alben, the State Police chief, briefed Patrick on Wednesday about the key piece of video showing Dzhokhar abandoning his backpack. Alben described the clip and showed the governor photographs culled from the footage, information that Patrick called "chilling."
>
> "We have a break," Patrick remembers him saying. "We think we have a face."
>
> If further proof was needed that the city was on edge, the anxiety soon spilled over into view. By 1 p.m., news reports began surfacing that a suspect had been not only identified but arrested, and was headed to the federal courthouse.

I'm still not satisfied with this explanation (and do hope Congress does some hearings on why facial recognition software failed to fulfill its promise, if in fact it did). But it does seem to suggest the FBI had solid images of the brothers for 18 hours before they released them to the public (a decision made by the FBI, the

BoGlo reports) and set off the manhunt that shut down the city.

Also, remember our questions about Ray Kelly's boast of having pictures of the Dzhokhar in Times Square, as the law enforcement community tried to use a half-baked plan to escape to New York and set off pressure cooker bombs in Times Square?

It appears from the coverage that the pictures derived not from NYC's ring of steel, but from the picture Dzhokhar put on Vkontakte. CBS national makes that explicit, and this image from CBS local admits the picture is a personal one.

Dzhokhar Tsarnaev in Times Square. (credit: Personal Photo)

The NYDN, in a story I won't link because of the way it identifies potentially innocent friends of Dzhokhar's who have been detained for visa violations, uses the same image.

In other words, Ray Kelly's Ring of Steel is no match for Dzhokhar's own (Russian) Facebook page, along with his Twitter account that described another trip to NYC.

Granted, fully-trained terrorists wouldn't be so sloppy with their social media use as this kid recruited by his brother just before the attack.

But in this instance, Facebook appears to have been just as important a surveillance tool as all the private videos that gave pictures, but reportedly not the ID, of the brothers.

Update: I meant to mention this bit from the

BoGlo article, too.

> The global positioning system on the vehicle, which emitted tiny traceable electronic signals, showed that the Mercedes was less than 5 miles from their apartment — and heading Reynolds's way.

It suggests, as I've wondered about repeatedly, that it was the Mercedes' location device, not the hostage's phone, that alerted the cops to where the SUV was.

COX ON ROGERS: "LIKE HE WAS J. EDGAR HOOVER"

Since Carl Levin announced he would retire, I've been hoping to see Justin Amash take on Mike Rogers in a Republican primary. This National Journal article captures the dynamics of that possibility well (though may overestimate how much money Amash could raise).

But before I get into why I'd be so fascinated about such a race, check out how former Republican Attorney General Mike Cox describes Mike Rogers.

> If Rogers were to run, he would have to give up his chairmanship of the House Intelligence Committee, for which there are no term limits. Former GOP Michigan Attorney General Mike Cox downplayed that motivation, saying Rogers' ambition for higher office trumps his desire to make a meaningful influence in foreign policy. "If [Rogers] lost, he could make a lot of money in D.C. as a lobbyist,"

> Cox said last week. “He’s so full of [expletive] to begin with. He tells all these stories about being an FBI agent, and he was in the FBI for two years. Like he was J. Edgar Hoover.”

“He’s so full of shit to begin with.”

This is the great hope of MI’s GOP to take over Levin’s seat.

Now, Gary Peters, who’ll run on the Democratic side, is one of MI’s rising Democratic stars. And as the article notes, he hails from Oakland County, which is critical not just because of the fundraising base there, but because it’s the second largest county and pretty evenly split; Peters has a proven ability to win that critical swing county’s votes.

Nevertheless, in spite of the fact that if Amash ran (whether or not he won), I’d probably end up represented by a GOP neanderthal rather than Amash (because Democrats are unlikely to win the district in an off year, and because there are tons of up-and-coming neanderthal GOPers in the Grand Rapids area), I’d still really like to see a Rogers-Amash race.

That’s because it’d serve as a nationally watched race between the GOP’s rising libertarian wing and one of the GOP’s most authoritarian leaders. Mike Rogers has championed CISPA and whatever other new surveillance efforts anyone wanted. Justin Amash led those few Republicans who opposed it. Amash even came out in favor of reading Dzhokhar Tsarnaev a Miranda warning this weekend.

In other words, in a battle between Rogers and Amash, civil liberties and the Constitution would be central.

Mike Cox was making fun of Rogers’ self-promotion when he drew the analogy with J. Edgar (and there’s an implicit respect for Hoover in his comment). But it’s high time someone started making the analogy between the fear-mongering

and surveillance Rogers and others embrace and Hoover's.

TAMERLAN TSARNAEV PLACED IN DATABASE PERCEIVED AS WEAK, EVEN BY DHS

As the blame game starts on the Boston Marathon bombing, someone (maybe a blabby Senator?) made it public that the CIA asked to have Tamerlan Tsarnaev added to the Terrorist Identities Datamart Environment (TIDE) database last year.

> The CIA asked the main U.S. counterterrorism agency to add the name of one of the suspected Boston Marathon bombers to a watch list more than a year before the attack, according to U.S. officials.
>
> The agency took the step after Russian authorities contacted officials there in the fall of 2011 and raised concerns that Tamerlan Tsarnaev — who was killed last week in a confrontation with police — was seen as an increasingly radical Islamist and could be planning to travel overseas. The CIA requested that his name be put on a database maintained by the National Counterterrorism Center.
>
> That database, the Terrorist Identities Datamart Environment, or TIDE, is a data storehouse that feeds a series of government watch lists, including the FBI's main Terrorist Screening Database and the Transportation Security Administration's "no-fly" list.
>
> Officials said Tsarnaev's name was added

> to the database but it's unclear which agency added it.

We got a look at the TIDE database last year when Tom Coburn reviewed whether fusion centers do useful work. Here's what that report said about TIDE:

> While reporting information on an individual who is listed in the TIDE database sounds significant, the Subcommittee found that DHS officials tended to be skeptical about the value of such reporting, because of concerns about the quality of data contained in TIDE.156
>
> 156 Although NCTC describes its TIDE database as holding information on the identities of known and suspected terrorists, DHS officials – who interacted with TIDE data on a daily basis, as they reviewed reporting not only from state and local law enforcement encounters but from encounters by DHS components – said they found otherwise. "Not everything in TIDE is KST," DHS privacy official Ken Hunt told the Subcommittee, using a shorthand term for "known or suspected terrorist."
>
> "Would you buy a Ford?" one DHS Senior Reports Officer asked the Subcommittee staff during an interview, when he was asked how serious it was for someone to be a match to a TIDE record. "Ford Motor Company has a TIDE record."
>
> [snip]
>
> Ole Broughton headed Intelligence Oversight at I&A from September 2007 to January 2012. In an interview with the Subcommittee, Mr. Broughton expressed the concern DHS intelligence officials felt working with TIDE data. In one instance, Mr. Broughton recalled he "saw an individual's two-year-old son

> [identified] in an [Homeland Intelligence Report]. He had a TIDE record." Mr. Broughton believed part of the problem was that intelligence officials had routinely put information on "associates" of known or suspected terrorists into TIDE, without determining that that person would qualify as a known or suspected terrorist. "We had a lot of discussion regarding 'associates' in TIDE," Mr. Broughton said.
>
> [my emphasis]

This is not to say that Tamerlan shouldn't be in TIDE.

Rather, it says there's so much other crap in TIDE, that it isn't perceived as very useful — at least not by the people at DHS the Permanent Subcommittee on Investigations interviewed.

This is the problem with overcollection of data: it adds a bunch more hay to the haystack for the time you want to start looking for a needle.