CHAPO ESCAPES

Yesterday, once and future Sinaloa kingpin Chapo Guzmán escaped from the high security Mexican prison where he had been held since February 2014. He escaped via the same kind of highly developed tunnel system in which Mexican Naval forces, assisted by US Marshals and DEA Agents, found him. Both tunnels provided escapes through the bathroom.

You'd think maybe Mexican officials would have been on the lookout for any tunneling systems that might assist Guzmán.

Already, the Mexican press is calling this an embarrassment for Enrique Peña Nieto (though remember, he seemed rather reluctant to boast of Chapo's capture when it happened, until the story leaked to the US press).

US officials, who have curiously been granted anonymity to bitch, are complaining that the Mexicans never extradited Guzmán so we could dump him in Florence SuperMax, where he'd be far less likely to escape. The on-the-record statements from people like Attorney General Lynch are much more reserved — though even she makes it clear she wants to bring him here and try him.

I'm at least as interested in what this escape says about the hierarchy of the Mexican drug industry as anything about the legend of Chapo. WaPo's story — whose reporter is also tweeting some fascinating pictures that show just how predictable this escape should have been — also addressed this somewhat.

> Even with Guzman in jail, his Sinaloa organization remained the dominant narcotics smuggling power in Mexico, with trafficking networks that spread across the United States. Guzman's cartel sends more cocaine and marijuana than any other into the United States, according to DEA officials, and it accounts for more than half of the

> heroin surging into U.S. communities as overdose deaths skyrocket.
>
> [snip]
>
> Guzman's longtime business partner, Ismael "El Mayo" Zambada, was believed to have assumed operational control of the cartel after Guzman's arrest, though few in Mexico doubted that Chapo continued calling the shots from his maximum-security cell.

That is, Chapo's arrest seems to have had little affect on the dominance of Sinaloa in the market (which may also suggest some favor from officials). Which will likely lead the decapitation-faithful in US law enforcement agencies to accidentally shoot Guzmán the next time we "help" with an arrest.

Finally, Chapo's escape has led to predictable tut-tutting about the corruption of Mexico generally and Peña Nieto specifically. Those complaints are true: over time we're likely to discover that Guzmán had help from inside, if not from even higher-level authorities (the house where his tunnel ended is close to a military base, apparently).

But is the US really in any position to complain? After all, at least under Eric Holder, our government didn't even *try* to imprison our transnational crime organization bosses — people like Jamie Dimon and Lloyd Blankfein, men who don't use the same overt violence that Sinaloa does, but who nevertheless have presided over transnational networks of entrenched crime. Jamie Dimon has never had to hide in a tunnel, in part because DOJ presumed he'd always escape whatever legal efforts we made to keep him there. And one reason we don't change the underlying law is because our Presidents, of both parties, are just as tied to those criminal TCOs as Peña Nieto and many of his predecessors.

I absolutely agree that Guzmán's escape reflects the lack of seriousness of some in Mexico about

prosecuting him. But that's not unique to Mexico, not even in North America.

THE GOVERNMENT CHANGED ITS MIND ABOUT HOW MANY DATABASES IT SEARCHED IN THE HASSANSHAHI CASE AFTER IT SHUT DOWN THE DEA DRAGNET

As I noted in this post, the government insists that it did not engage in parallel construction in the case of Shantia Hassanshahi, the Iranian-American busted for sanctions violations using evidence derivative of a search of what the government now claims was a DEA dragnet. "While it would not be improper for a law enforcement agency to take steps to protect the confidentiality of a law enforcement sensitive investigative technique, this case raises no such issue."

The claim is almost certainly bullshit, true in only the narrowest sense.

Indeed, the changing story the government has offered about how they IDed Hassanshahi based off a single call he had with a phone belonging to a person of interest, "Sheikhi," in Iran, is instructive not just against the background of the slow reveal of multiple dragnets over the same period. But also for the technological capabilities included in those claims. Basically, the government appears to be claiming they got a VOIP call from a telephony database.

As I lay out below, the story told by the government in various affidavits and declarations (curiously, the version of the first one that appears in the docket is not signed) changed in multiple ways. While there were other changes, the changes I'm most interested in pertain to:

- Whether Homeland Security Investigator Joshua Akronowitz searched just one database — the DEA toll record database — or multiple databases
- How Akronowitz identified Google as the provider for Hassanshahi's phone record
- When and how Akronowitz became interested in a call to Hassanshahi from another Iranian number
- How many calls of interest there were

As you can see from the excerpts below, Akronowitz at first claimed to have searched "HSI-accessible law enforcement databases," plural, and suggested he searched them himself. In July 2014, in response to a motion to suppress (and after Edward Snowden had disclosed the NSA's phone dragnet), Akronowitz changed that story and said he *sent a research request* to a single database, implying someone else did a search of just one database. Akronowitz told the same story in yet another revised affidavit submitted last October. In the declaration submitted in December but unsealed in January, DEA Assistant Special Agent Robert Patterson stuck with the single database story and used the passive voice to hide who did the database query.

While Akronowitz' story didn't change regarding

how he discovered that Hassanshahi's phone was a Google number, it did get more detailed in the July 2014 affidavit, which explained that he had first checked with another VOIP provider before being referred to Google.

Perhaps most interestingly, the government's story changed regarding how many calls of interest there were, and between what numbers. In January 2013, Akronowitz said "a number of telephone calls between 'Sheikhi's' known business telephone number and telephone number 818-971-9512 had occurred within a relatively narrow time frame" (though he doesn't tell us what that time frame was). He also says that his Google subpoena showed "numerous calls to the same Iranian-based telephone number during a relatively finite period of time." He neither explained that this number was not Sheikhi's number — it was a different Iranian number — nor what he means by "a relatively finite period of time." His July and October affidavits said his research showed a contact, "on one occasion, that is, on July 4, 2011," with Sheikhi's number. The July affidavit maintained the claim that there were multiple calls between Hassanshahi's number and an Iranian one: "numerous phone calls between Hassanshahi's '818' number and one Iranian phone number." But by October, Akronowitz conceded that the Google records showed only "that Hassanshahi's '818' number made contact with an Iranian phone number (982144406457) only once, on October 5, 2011" (as well as a "22932293" number that he bizarrely claimed was a call to Iran). Note, Akronowitz' currently operative story would mean the government never checked whether there were any calls between Hassanshahi and Sheikhi between August 24 and September 6 (or after October 6), which would be rather remarkable. Patterson's December affidavit provided no details about the date of the single call discovered using what he identified as DEA's database, but did specify that the call was made by Hassanshahi's phone, outbound to Iran. (Patterson didn't address the later Google production, as that was pursuant to a subpoena.)

To sum up, before Edward Snowden's leaks alerted us to the scope of NSA's domestic and international dragnet, Akronowitz claimed *he personally* had searched multiple databases and found evidence of multiple calls between Hassanshahi's phone number and Sheikhi's number, as well as (after getting a month of call records from Google) multiple calls to another Iranian number over unspecified periods of time. After Snowden's leaks alerted us to the dragnet, after Dianne Feinstein made it clear the NSA can search on Iranian targets in the Section 215 database, which somehow counts as a terrorist purpose, and after Eric Holder decided to shut down *just the DEA dragnet*, Akronowitz changed his story to claim he had found just one call between Hassanshahi and Shiekhi, and — after a few more months — just one call from another Iranian number to Hassanshahi. Then, two months later, the government claimed that the only database that ever got searched was the DEA one (the one that had already been shut down) which — Patterson told us — was based on records obtained from "United States telecommunications service providers" via a subpoena.

Before I go on, consider that the government currently claims it used just a single phone call of interest — and the absence of any additional calls in a later months's worth of call records collected that fall — to conduct a warrantless search of a laptop in a state (CA) where such searches require warrants, after having previously claimed there was a potentially more interesting set of call records to base that search on.

Aside from the government's currently operative claim that it would conduct border searches based on the metadata tied to a single phone call, I find all this interesting for two reasons.

First, the government's story about how many databases got searched and how many calls got found changed in such a way that the only

admission of an unconstitutional search to the judge, in December 2014, involved a database that had allegedly been shut down 15 months earlier.

Maybe they're telling the truth. Or maybe Akronowitz searched or had searched multiple databases — as he first claimed — and found the multiple calls he originally claimed, but then revised his story to match what could have been found in the DEA database. We don't know, for example, if the DEA database permits "hops," but he might have found a more interesting call pattern had he been able to examine hops (for example, it might explain his interest in the *other* phone number in Iran, which otherwise would reflect no more than an immigrant receiving a call from his home country).

All of this is made more interesting because of my second point: *the US side of the call in question was an Internet call*, a Google call, not a telephony call. Indeed, at least according to Patterson's declaration (records of this call weren't turned over in discovery, as far as I can tell), Hassanshahi placed the call, not Sheikhi.

I have no idea how Google calls get routed, but given that Hassanshahi placed the call, there's a high likelihood that it didn't cross a telecom provider's backbone in this country (and god only knows how DEA or NSA would collect Iranian telephony provider records), which is who Patterson suggests the calls came from (though there's some room for ambiguity in his use of the term "telecommunications service providers").

USAT's story on this dragnet suggests the data all comes from *telephone* companies.

> It allowed agents to link the call records its agents gathered domestically with calling data the DEA and intelligence agencies had acquired outside the USA. (In some cases,

> officials said the DEA paid employees of foreign telecom firms for copies of call logs and subscriber lists.)
>
> [snip]
>
> Instead of simply asking phone companies for records about calls made by people suspected of drug crimes, the Justice Department began ordering telephone companies to turn over lists of all phone calls from the USA to countries where the government determined drug traffickers operated, current and former officials said.
>
> [snip]
>
> Former officials said the operation included records from AT&T and other telecom companies.

But if this call really was placed from a Google number, it's not clear it would come up under such production, even under production of calls that pass through telephone companies' backbones. That may reflect — if the claims in this case are remotely honest — that the DEA dragnet, at least, gathered call records not just from telecom companies, but also from Internet companies (remember, too, that DOJ's Inspector General has suggested DEA had or has more than one dragnet, so it may also have been collecting Internet toll records).

And that — coupled with the government's evolving claims about how many databases got checked and how many calls that research reflected — may suggest something else. Given that the redactions on the providers obliged under the Section 215 phone dragnet orders haven't changed going back to 2009, when it was fairly clear there were just 3 providers (AT&T, Sprint, and Verizon), it may be safe to assume that's still all NSA collects from. A never-ending series of leaks have pointed out that the 215 phone dragnet increasingly has gaps in coverage. And this Google call would be

precisely the kind of call we would expect it to miss (indeed, that's consistent with what Verizon Associate General Counsel — and former DOJ National Security Division and FBI Counsel — Michael Woods testified to before the SSCI last year, strongly suggesting the 215 dragnet missed VOIP). So while FISC has approved use of the "terrorist" Section 215 database for the terrorist group, "Iran," (meaning NSA might actually have been able to query on Sheikhi), we should expect that this call would not be in that database. Mind you, we should also expect NSA's EO 12333 dragnet — which permits contact chaining on US persons under SPCMA — to include VOIP calls, even with Iran. But depending on what databases someone consulted, we would expect gaps in precisely the places where the government's story has changed since it decided it had searched only the now-defunct DEA database.

Finally, note that if the government was sufficiently interested in Sheikhi, it could easily have targeted him under PRISM (he did have a GMail account), which would have made any metadata tied to any of his Google identities broadly shareable within the government (though DHS Inspectors would likely have to go through another agency, quite possibly the CIA). PRISM production should return any Internet phone calls (though there's nothing in the public record to indicate Sheikhi had an Internet phone number). Indeed, the way the NSA's larger dragnets work, a search on Sheikhi would chain on all his correlated identifiers, including any communications via another number or Internet identifier, and so would chain on whatever collection they had from his GMail address and any other Google services he used (and the USAT described the DEA dragnet as using similarly automated techniques). In other words, when Akronowitz originally said there had been multiple "telephone calls," he may have instead meant that Sheikhi and Hassanshahi had communicated, via a variety of different identifiers, multiple times as reflected in his search (and given what we know about DEA's phone

dragnet and my suspicion they also had an Internet dragnet, that might have come up just on the DEA dragnets alone).

The point is that each of these dragnets will have slightly different strengths and weaknesses. Given Akronowitz' original claims, it sounds like he may have consulted dragnets with slightly better coverage than just the DEA phone dragnet — either including a correlated DEA Internet dragnet or a more extensive NSA one — but the government now claims that it only consulted the DEA dragnet and consequently claims it only found one call, a call it should have almost no reason to have an interest in.

January 9, 2013:

15. Using the business telephone number associated with "Sheikhi", I searched HSI-accessible law enforcement databases, in furtherance of identifying potential U.S.-based targets engaged in the sale or export of protection relays for use in the Iranian electrical power grid. As a result of my search, I discovered telephone call log records indicating that a number of telephone calls between "Sheikhi's" known business telephone number and telephone number 818-971-9512 had occurred within a relatively narrow time frame. Based on my training and experience, I know that area code "818" is an area code originating in Los Angeles County, CA.

16. On or about October 6, 2011, I prepared and served an Administrative Export Enforcement Subpoena for subscriber information for telephone number 818-971-9512 on Google, Inc. ("Google"), the U.S.-based service provider. In response, Google produced the following subscriber information for the telephone number:

Name: Shantia HASSANSHAHI

E-mail: [my redaction]@gmail.com

Address: [my redaction]

Alt Phone Number: 805-857-4669

Created on: 2010 Jun 17 09:52:20

Signup IP: 72.134.19.172

In addition, Google produced call log information for the telephone number during the period of September 6, 2011, to October 6, 2011, which revealed numerous outgoing calls made to telephone number 98-938-1911602. Again, based on my training and experience, I know that the country code for the Islamic Republic of Iran is "98." Accordingly, it appeared that HASSANSHAHI, using a U.S.-based telephone number suspected of having a connection to the suspected procurement network (i.e., 818-971- 9512), made numerous calls to the same Iranian-based telephone number during a relatively finite period of time.

July 9, 2014

On August 24, 2011, I sent a research request for information on phone number 982144406457, which is an Iranian phone number that was included in Sheikhi's signature block in the email he sent to the source. The research request was sent to an HSI-accessible law enforcement database.

On August 24, 2011, I reviewed the research provided in response to my request , which revealed that the Iranian phone number had been in contact with a domestic phone number, 818-971-9512, on one occasion, that is, on July 4, 2011. At the time I reviewed the response, the "818" number was the only U.S. phone number that had been in contact with the Iranian phone number. Based on my professional experience, because I once worked in Los Angeles, California, I recognized the "818" area code was assigned to the Los Angeles County area. My request did not yield any other information that was useful to my investigation.

[snip]

On September 27, 2011, I performed a Google

internet search on the “818” phone number to find out which phone company was assigned to that phone number. That open source internet search showed that the phone number was assigned to Bandwidth.com Inc. I then prepared and served an Administrative Export Enforcement Control Subpoena on Bandwidth.com Inc. to obtain subscriber and toll information for that phone number.

On October 4, 2011, I received a response from Bandwidth.com Inc., which stated that Bandwidth was not the service provider for the “818” number. Bandwidth’s response indicated that Google/Google Voice was the current provider.

On October 6, 2011, I prepared and served an Administrative Export Enforcement Subpoena on Google/Google Voice for subscriber and toll information for phone number 818-971-9512.

On October 18, 2011, Google responded to my subpoena request with subscriber information showing that the “818” number was registered to Shantia Hassanshahi, with a particular home address in Westlake Village, California. Google also provided call log information for the period of September 6, 2011 to October 6, 2011, which showed numerous phone calls between Hassanshahi’s “818” number and one Iranian phone number. Google’s response also identified Hassanshahi’s email address as [my redaction]@gmail.com.

October 14, 2014

On August 24, 2011, I sent a research request for information on phone number 982144406457, which is an Iranian phone number that was included in Sheikhi’s signature block in the email he sent to the source. The research request was sent to an HSI-accessible law enforcement database.

On August 24, 2011, I reviewed the research provided in response to my request , which revealed that the Iranian phone number had been

in contact with a domestic phone number, 818-971-9512, on one occasion, that is, on July 4, 2011. At the time I reviewed the response, the "818" number was the only U.S. phone number that had been in contact with the Iranian phone number. Based on my professional experience, because I once worked in Los Angeles, California, I recognized the "818" area code was assigned to the Los Angeles County area. My request did not yield any other information that was useful to my investigation.

[snip]

On September 27, 2011, I performed a Google internet search on the "818" phone number to find out which phone company was assigned to that phone number. That open source internet search showed that the phone number was assigned to Bandwidth.com Inc. I then prepared and served an Administrative Export Enforcement Control Subpoena on Bandwidth.com Inc. to obtain subscriber and toll information for that phone number.

On October 4, 2011, I received a response from Bandwidth.com Inc., which stated that Bandwidth was not the service provider for the "818" number. Bandwidth's response indicated that Google/Google Voice was the current provider.

On October 6, 2011, I prepared and served an Administrative Export Enforcement Subpoena on Google/Google Voice for subscriber and toll information for phone number 818-971-9512.

On October 18, 2011, Google responded to my subpoena request with subscriber information showing that the "818" number was registered to Shantia Hassanshahi, with a particular home address in Westlake Village, California. Google also provided call log information for the period of September 6, 2011 to October 6, 2011, which that Hassanshahi's "818" number made contact with an Iranian phone number (982144406457) only once, on October 5, 2011. In addition, there is a missed call between Hassanshahi's "818" number and an Iranian cell

phone number (22932293) on September 19, 2011. Google's response also identified Hassanshahi's email address as [my redaction]@gmail.com.

December 15, 2014 (unsealed January 15, 2015)

As described in the previously filed, public affidavit of Joshua J. Akronowitz, Government investigators learned that there was reason to believe that Iranian telephone number 982144406457 (hereinafter, "the Iranian number") was relevant to an ongoing federal criminal investigation. The Iranian number was queried in a federal law enforcement database [redacted] the database indicated that a call had been placed from the 818 number to the Iranian number.

This database [redacted] consisted of telecommunications metadata obtained from United States telecommunications service providers pursuant to administrative subpoenas served upon the service providers under the provisions of 21 U.S.C. § 876. This metadata related to international telephone calls originating in the United States and calling [redacted] designated foreign countries, one of which was Iran, that were determined to have a demonstrated nexus to international drug trafficking and related criminal activities. This metadata consisted exclusively of the initiating telephone number; the receiving telephone number; the date, time, and duration of the call; and the method by which the call was billed. No subscriber information or other personal identifying information was included in this database. No communication content was included in this database.

HASSANSHAHI BIDS TO UNDERMINE THE DEA DRAGNET … AND ALL DRAGNETS

Often forgotten in the new reporting on the DEA dragnet is the story of Shantia Hassanshahi, the Iranian-American accused of sanctions violations who was first IDed using the DEA dragnet. That's a shame, because his case may present real problems not just for the allegedly defunct DEA dragnet, but for the theory behind dragnets generally.

As I laid out in December, as Hassanshahi tried to understand the provenance of his arrest, the story the Homeland Security affiant gave about the database(s) he used to discover Hassanshahi's ties to Iran in the case changed materially, so Hassanshahi challenged the use of the database and everything derivative of it. The government, which had not yet explained what the database was, asked Judge Rudolph Contreras to assume the database was not constitutional, but to upheld its use and the derivative evidence anyway, which he did. At the same time, however, Contreras required the government to submit an explanation of what the database was, which was subsequently unsealed in January.

Not surprisingly, Hassanshahi challenged the use of a DEA database to find him for a crime completely unrelated to drug trafficking, first at a hearing on January 29. In response to an order from Contreras, the government submitted a filing arguing that Hassanshahi lacks standing to challenge the use of the DEA dragnet against him.

> To the extent that defendant seeks to argue that the administrative subpoenas to telephone providers violated the statutory requirements of Section

> 876(a), he clearly lacks standing to do so. See, e.g., United States v. Miller, 425 U.S. 435, 444 (1976) ("this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant"); Moffett, 84 F.3d at 1293-94 (defendant could not challenge a Section 876(a) subpoena to third party on the grounds that it exceeded the DEA's statutory authority).

This is the argument the government currently uses to deny defendants notice on Section 215 use.

The government further argued that precedent permits it to use information acquired for other investigations.

> DEA acquired information through use of its own investigatory techniques and for its own narcotics-related law enforcement purposes. DEA shared with HSI a small piece of this information to assist HSI in pursuing a non-narcotics law enforcement investigation. In doing so, DEA acted consistently with the longstanding legal rule that "[e]vidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken." Jabara v. Webster, 691 F.2d 272, 277 (6th Cir. 1982) (quotation marks omitted); accord United States v. Joseph, 829 F.2d 724, 727 (9th Cir. 1987).
>
> Applying an analogous principle, the D.C. Circuit has held that querying an existing government database does not constitute a separate Fourth Amendment search: "As the Supreme Court has held, the process of matching one piece of personal information against government

> records does not implicate the Fourth Amendment." Johnson v. Quander, 440 F.3d 489, 498 (D.C. Cir. 2006) (citing Arizona v. Hicks, 480 U.S. 321 (1987)). The D.C. Circuit observed that a contrary rule would impose "staggering" consequences, placing "an intolerable burden" on law enforcement if each query of a government database "were subject to Fourth Amendment challenges." Id. at 499.

This is a version of the argument the government has used to be able to do back door searches of Section 702 data.

It also argued there was no suppression remedy included in 21 USC 876, again a parallel argument it has made in likely Section 215 cases.

Finally, it also argued, in passing, that its parallel construction was permissible because, "While it would not be improper for a law enforcement agency to take steps to protect the confidentiality of a law enforcement sensitive investigative technique, this case raises no such issue." No parallel construction happened, it claims, in spite of changing stories in the DHS affidavit.

Yesterday, Hassanshahi responded. (h/t SC) In it, his attorneys distinguished the use of the DEA dragnet for purposes not permitted by the law — a systematic violation of the law, they argue — from the use of properly collected data in other investigations.

> Title 21 USC § 876 allows the government to serve an administrative subpoena in connection with a purely drug enforcement investigation. Government has systematically violated this statute for over a decade by using the subpoena process to secretly gather a database of telephony information on all Americans, and then utilizing the database (while

> disguising its source) in all manner of investigations in all fields not related to drugs at all.
>
> [snip]
>
> This was not a one-time or negligent statutory violation that happened to uncover evidence of another crime, or even the sharing of information legitimately gathered for one purpose with another agency. Cf. Johnson v. Quander, 440 F.3d 489 (D.C.Cir. 2006) (government may use DNA profiles gathered pursuant to and in conformance with statute for other investigations). By its very nature, the gathering of telephony information was repeated and systematic, as was the making available of the database to all government agencies, and all aspects of the scheme (from gathering to dissemination outside drug investigations) violated the statute.

But more importantly, Hassanshahi pointed to the government's request — from before they were ordered to 'fess up about this dragnet — that the Judge assume this dragnet was unconstitutional, to argue the government has already ceded the question of standing.

> Defendant herein submits that a systematic statutory violation, or a program whose purpose is to violate the statute continuously over decades, presents a case of first impression not governed by Sanchez-Llamas or other government cases.
>
> But the Court need not reach the novel issue because in the instant case, the government *already conceded* that use of the database was a constitutional violation of *Mr. Hassanshahi's rights*. Indeed the Court asked this Court to assume the constitutional violation.

> Mem. Dec. p. 9. Where there is a statutory violation plus an individual constitutional violation, the evidence shall be suppressed even under government's cited cases.
>
> [snip]
>
> Government now argues Mr. Hassanshahi "lacks standing" to contest the statutory violation. Again, government forgets it previously conceded that use of the database was unconstitutional, meaning unconstitutional *as to defendant* (otherwise the concession was meaningless and afforded no grounds to withhold information). Mr. Hassanshahi obviously has standing to assert a conceded constitutional violation. [emphasis original]

In short, Hassanshahi is making a challenge to the logic behind this and a number of other dragnets, or demanding the judge suppress the evidence against him (which would almost certainly result in dismissal of the case).

We'll see how Contraras responds to all this, but given that he has let it get this far, he may be sympathetic to this argument.

In which case, things would get fun pretty quickly. Because you'd have a defendant *with standing* arguing not just that the use of the DEA dragnet for non-DEA uses was unconstitutional, but also that all the arguments that underly the use of the phone dragnet and back door searches were unconstitutional. And he'd be doing so in the one circuit with a precedent on mosaic collection that could quickly get implicated here. This case, far more than even the ACLU lawsuit against the Section 215 database (but especially the Smith and Klayman challenges), and even than Basaaly Moalin's challenge to the use of the 215 dragnet against him, would present real problems for the claims to dragnet

legally.

In other words, if this challenge were to go anywhere, it would present big problems not only for other uses of the DEA dragnet, but also, possibly, for the NSA dragnets.

Mind you, there is no chance in hell the government would let it get that far. They'd settle with Hassanshahi long before they permitted that to happen in a bid to find a way to bury this DEA dragnet once and for all and retain their related arguments for use with the NSA dragnets and related collection.

But we might get the dragnetters sweat just a bit.

DEA'S DRAGNET AND DAVID HEADLEY

In a piece on the DEA dragnet the other day, Julian Sanchez made an important point. The existence of the DEA dragnet — and FBI's use of it in previous terrorist attacks — destroys what little validity was left of the claim that NSA needed the Section 215 dragnet after 9/11 to close a so-called "gap" they had between a safe house phone in Yemen and plotters in the US (though an international EO 12333 database would have already proven that wrong).

> First, the program's defenders often suggest that had we only had some kind of bulk telephone database, the perpetrators of the 9/11 attacks could have been identified via their calls to a known safehouse in Yemen. Now, of course, we know that there *was* such a database—and indeed, a database that had already been employed in other counterterror investigations, including the 1995 Oklahoma City bombing. It does

> not appear to have helped.

But the DEA dragnet is even more damning for another set of claims, and for another terrorist attack such dragnets failed to prevent: former DEA informant David Headley, one of the key planners of the 2008 Mumbai attack.

Headley provided DEA the phone data they would have needed to track him via their dragnet

As ProPublica extensively reported in 2013, Headley first got involved in Lashkar-e-Taiba while he remained on the DEA's payroll, at a time when he was targeting Pakistani traffickers. Indeed, after 9/11, his DEA handler called him for information on al Qaeda. All this time, Headley was working phone based sources.

> Headley returned to New York and resumed work for the DEA in early 2000. That April, he went undercover in an operation against Pakistani traffickers that resulted in the seizure of a kilo of heroin, according to the senior DEA official.
>
> At the same time, Headley immersed himself in the ideology of Lashkar-i-Taiba. He took trips to Pakistan without permission of the U.S. authorities. And in the winter of 2000, he met Hafiz Saeed, the spiritual leader of Lashkar.
>
> Saeed had built his group into a proxy army of the Pakistani security forces, which cultivated militant groups in the struggle against India. Lashkar was an ally of al Qaeda, but it was not illegal in Pakistan or the United States at the time.
>
> [snip]
>
> Headley later testified that he told his

> DEA handler about his views about the disputed territory of Kashmir, Lashkar's main battleground. But the senior DEA official insisted that agents did not know about his travel to Pakistan or notice his radicalization.
>
> On Sept. 6, 2001, Headley signed up to work another year as a DEA informant, according to the senior DEA official.
>
> On Sept. 12, Headley's DEA handler called him.
>
> Agents were canvassing sources for information on the al Qaeda attacks of the day before. Headley angrily said he was an American and would have told the agent if he knew anything, according to the senior DEA official.
>
> Headley began collecting counterterror intelligence, according to his testimony and the senior DEA official. He worked sources in Pakistan by phone, getting numbers for drug traffickers and Islamic extremists, according to his testimony and U.S. officials.

Even at this early stage, the FBI had a warning about Headley, via his then girlfriend who warned a bartender Headley had cheered the 9/11 attack; the bartender passed on the tip. And Headley was providing the DEA — which already had a dragnet in place — phone data on his contacts, including Islamic extremists, in Pakistan.

ProPublica's sources provide good reason to believe DEA, possibly with the FBI, sent Headley to Pakistan even after that tip, and remained an informant until at least 2005.

So the DEA (or whatever agency had sent him) not only *should have been able to* track Headley and those he was talking to using their dragnet, but they were using him to get phone contacts they could track (and my understanding is that

agreeing to be an informant amounts to consent to have your calls monitored, though see this post on the possible "defeat" of informant identifiers).

Did Headley's knowledge of DEA's phone tracking help the Mumbai plotters avoid detection?

Maybe. And/or maybe Headley taught his co-conspirators how to avoid detection.

Of course, Headley could have just protected some of the most interesting phone contacts of his associates (but again, DEA should have tracked who he was talking to if they were using him to collect telephony intelligence).

More importantly, he may have alerted Laskar-e-Taiba to phone-based surveillance.

In a December joint article with the NYT, ProPublica provided details on how one of Headley's co-conspirators, Zarrar Shah, set up a New Jersey-based VOIP service so it would appear that their calls were originating in New Jersey.

> Not long after the British gained access to his communications, Mr. Shah contacted a New Jersey company, posing online as an Indian reseller of telephone services named Kharak Singh, purporting to be based in Mumbai. His Indian persona started haggling over the price of a voice-over-Internet phone service — also known as VoIP — that had been chosen because it would make calls between Pakistan and the terrorists in Mumbai appear as if they were originating in Austria and New Jersey.
>
> "its not first time in my life i am perchasing in this VOIP business," Mr. Shah wrote in shaky English, to an official with the New Jersey-based company when he thought the asking price

> was too high, the GCHQ documents show. "i am using these services from 2 years."
>
> Mr. Shah had begun researching the VoIP systems, online security, and ways to hide his communications as early as mid-September, according to the documents.
>
> [snip]
>
> Eventually Mr. Shah did set up the VoIP service through the New Jersey company, ensuring that many of his calls to the terrorists would bear the area code 201, concealing their actual origin.

We have reason to believe that VOIP is one of the gaps in *all* domestic-international dragnets that agencies are just now beginning to close. And by proxying through the US, those calls would have been treated as US person calls (though given the clear foreign intelligence purpose, they would have met any retention guidelines, though may have been partly blocked in CIA's dragnet). While there's no reason to believe that Headley knew that, he likely knew what kind of phone records his handlers had been most interested in.

But it shouldn't have mattered. As the article makes clear, GCHQ not only collected the VOIP communications, but Shah's communications as he set them up.

Did FBI claim it tracked Headley using the NSA dragnet when it had actually used the DEA one?

I've been arguing for years that if dragnet champions want to claim they work, they need to explain why they point to Headley as a success story because they prevented his planned attack on a Danish newspaper, when they failed to prevent the even more complex Mumbai attack.

Nevertheless, they did claim it — or at least strongly suggest it — as a success, as in FBI Acting Assistant Director Robert Holley's sworn declaration in *Klayman v. Obama*.

> In October 2009, David Coleman Headley, a Chicago businessman and dual U.S. and Pakistani citizen, was arrested by the FBI as he tried to depart from Chicago O'Hare airport on a trip to Pakistan. At the time of his arrest, Headley and his colleagues, at the behest of al-Qa'ida, were plotting to attack the Danish newspaper that published cartoons depicting the Prophet Mohammed. Headley was later charged with support for terrorism based on his involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Collection against foreign terrorists and telephony metadata analysis were utilized in tandem with FBI law enforcement authorities to establish Headley's foreign ties and put them in context with his U.S. based planning efforts.

That said, note how Holley doesn't specifically invoke Section 215 (or, for that matter, Section 702, which the FBI had earlier claimed they used against Headley)?

Now compare that to what the Privacy and Civil Liberties Oversight Board said about the use of Section 215 against Headley.

> In October 2009, Chicago resident David Coleman Headley was arrested and charged for his role in plotting to attack the Danish newspaper that published inflammatory cartoons of the Prophet Mohammed. He was later charged with helping orchestrate the 2008 Mumbai hotel attack, in collaboration with the Pakistan-based militant group Lashkar-e-Taiba. He pled guilty and began cooperating with authorities.

> Headley, who had previously served as an informant for the Drug Enforcement Agency, was identified by law enforcement as involved in terrorism through means that did not involve Section 215. Further investigation, also not involving Section 215, provided insight into the activities of his overseas associates. In addition, Section 215 records were queried by the NSA, which passed on telephone numbers to the FBI as leads. Those numbers, however, only corroborated data about telephone calls that the FBI obtained independently through other authorities.
>
> Thus, we are aware of no indication that bulk collection of telephone records through Section 215 made any significant contribution to the David Coleman Headley investigation.

First, by invoking Headley's role as an informant, PCLOB found reason to focus on DEA right before they repeatedly point to other authorities: Headley was IDed by "law enforcement" via means that did not involve 215, his collaborators were identified via means that did not involve 215, and when they finally did query 215, they only "corroborated data about telephone calls that the FBI had obtained independently through other authorities."

While PCLOB doesn't say any of these other authorities *are* DEA's dragnet, all of them could be (though some of them could also be NSA's EO 12333 dragnet, or whatever dragnet CIA runs, or GCHQ collection, or Section 702, or — some of them — FBI NSL-based collection, or tips). What does seem even more clear now than when PCLOB released this is that NSA was trying to claim credit for someone else's dragnet, so much so that even the FBI itself was hedging claims when making sworn declarations.

Of course, whatever dragnet it was that identified Headley's role in Laskar-e-Taiba,

even the DEA's own dragnet failed to identify him in the planning stage for the larger of the attacks.

If the DEA's own dragnet can't find its own informant plotting with people he's identified in intelligence reports, how successful is any dragnet going to be?

A GUIDE TO THE 5+ KNOWN INTELLIGENCE COMMUNITY TELECOMMUNICATIONS METADATA DRAGNETS

I've been laying this explanation out since USA Today provided new details on DEA's International Dragnet, but it's clear it needs to be done in more systematic fashion, because really smart people continue to mistakenly treat the Section 215 database as the analogue to the DEA dragnet described by USAT, which it's not. There are at least five known telecommunications dragnets (some of which appear to integrate other kinds of metadata, especially Internet metadata). Here's a quick guide to what is known about each (click to enlarge, let me know of corrections/additions, I will do running updates to make this more useful):

	NSA	DEA	CIA	FBI
International	**EO 12333 / SPCMA** • Includes Internet metadata • Analysts need only FI purpose, including CN • Since 2008 permitted chaining on USPs, but not targeting them • Standard minimization procedures • Chains across metadata type • Linked into automatic analysis • Probably includes location data	**USTO: 21 USC 876** (DEA's "tangible things" subpoenas) • Ostensibly counternarcotics purpose, but used for other purposes (included counterproliferation) • Linked into automatic analysis • Location data inclusion unclear • Allegedly shut down in September 2013	**PROTON** (predecessor to ICREACH) Chains across metadata type **AT&T** voluntary production of foreign calls	
Domestic	**Section 215** • Limited to counterterrorism purpose • Strict dissemination limitations • First Amendment review for chaining • Chaining permitted on USPs • Linked into automatic analysis until 2009; NSA has given up effort to return to automatic chaining • Currently limited to pre-approved or emergency queries (~300 identifiers queried multiple times)	**Hemisphere** (provider based, may be limited to AT&T backbone) • Ostensibly counternarcotics purpose, but used by other agencies • Includes analysis involving location data		**Exigent Letters** Onsite telecom presence from 2002-2006 Ongoing **TCAU** contracts with AT&T and another telecom; AT&T provides enhanced services

NSA, International

When people think about the NSA dragnet they mistakenly think exclusively of Section 215. That is probably the result of a deliberate strategy from the government, but it leads to gross misunderstanding on many levels. As Richard Clarke said in Congressional testimony last year, Section "215 produces a small percentage of the overall data that's collected."

Like DEA, NSA has a dragnet of international phone calls, including calls into the United States. This is presumably limited only by technical capability, meaning the only thing excluded from this dragnet are calls NSA either doesn't want or that it can't get overseas (and note, some domestic cell phone data may be available offshore because of roaming requirements). David Kris has said that what collection of this comes from domestic providers comes under 18 U.S.C. § 2511(2)(f). And this dragnet is not just calls: it is also a whole slew of Internet data (because of the structure of the Internet, this will include a great deal of US person data). And it surely includes a lot of other data points, almost certainly including location data. Analysts can probably access Five Eyes and other intelligence partner data, though this likely includes additional restrictions.

There are, within this dragnet, two sets of procedures for accessing it. There is straight EO 12333, which appears to defeat US person data

(so if you're contact chaining and a known US person is included in the chain, you won't see it). This collection requires only a foreign intelligence purpose (which counternarcotics is explicitly included in). Standard NSA minimization procedures apply, which — given that this is not supposed to include US person data — are very permissive.

Starting in 2008 (and probably before 2004, at least as part of Stellar Wind), specially-trained analysts are also permitted to include US persons in the contact chaining they do on EO 12333 data, under an authority call "SPCMA" for "special procedures." They can't *target* Americans, but they can analyze and share US person data (and NSA has coached analysts how to target a foreign entity to get to the underlying US data). This would be treated under NSA's minimization procedures, meaning US person data may get masked unless there's a need for it. Very importantly, this chaining is not and never was limited to counterterrorism purposes — it only requires a foreign intelligence purpose. Particularly because so much metadata on Americans is available overseas, this means NSA can do a great deal of analysis on Americans without any suspicion of criminal ties.

Both of these authorities appear to link right into other automatic functions, including things like matching identities (such that it would track "emptywheel" across all the places I use that as my uniquename) and linking directly up to content, if it has been collected.

NSA, Domestic

Then there is the Section 215 dragnet, which prior to 2006 was conducted with telecoms voluntarily producing data but got moved to Section 215 thereafter; there is a still-active Jack Goldsmith OLC opinion that says the government does not need any additional statutory authorization for the dragnet (though telecoms aside from AT&T would likely be reluctant to do so now without liability protection and compensation).

Until 2009, the distinctions between NSA's EO 12333 data and Section 215 were not maintained. Indeed, in early 2008 "for purposes of analytical efficiency," the Section 215 data got dumped in with the EO 12333 data and it appears the government didn't even track data source (which FISC made them start doing by tagging each discrete piece of data in 2009), and so couldn't apply the Section 215 rules as required. Thus, until 2009, the Section 215 data was subjected to the automatic analysis the EO 12333 still is. That was shut down in 2009, though the government kept trying to find a way to resume such automatic analysis. It never succeeded and finally gave up last year, literally on the day the Administration announced its decision to move the data to the telecoms.

The Section 215 phone dragnet can only be used for counterterrorism purposes and any data that gets disseminated outside of those cleared for BRFISA (as the authority is called inside NSA) must be certified as to that CT purpose. US person identifiers targeted in the dragnet must

first be reviewed to ensure they're not targeted exclusively for First Amendment reasons. Since last year, FISC has pre-approved all identifiers used for chaining except under emergencies. Though note: Most US persons approved for FISA content warrants are automatically approved for Section 215 chaining (I believe this is done to facilitate the analysis of the content being collected).

Two very important and almost universally overlooked points. First, analysts access (or accessed, at least until 2011) BRFISA data from the very same computer interface as they do EO 12333 data (see above, which would have dated prior to the end of 2011). Before a chaining session, they just enter what data repositories they want access to and are approved for, and their analysis will pull from all those repositories. Chaining off data from more than one repository is called a "federated" query. And the contact chaining they got — at least as recently as 2011, anyway — also included data from both EO 12333 collection and Section 215 collection, both mixed in together. Importantly, data with one-end in foreign will be redundant, collected under both EO 12333 and 215. Indeed, a training program from 2011 trained analysts to re-run BRFISA queries that could be replicated under EO 12333 so they could be shared more permissively. That said, a footnote (see footnote 13) in phone dragnet orders that has mostly remained redacted appears to impose the BRFISA handling rules on any data comingled with it, so this may limit (or have imposed new more recent limits) on contact chaining between authorities.

As I noted, NSA shut down the automatic features on BRFISA data in 2009. But once data comes back in a query, it can be subjected to NSA's "full range of analytical tradecraft," as every phone dragnet order explains. Thus, while the majority of Americans who don't come up in a query don't get subjected to more intrusive analysis, if you're 3 hops (now 2) from someone of interest, you can be — everything, indefinitely. I would

expect that to include trolling all of NSA's collected data to see if any of your other identifiable data comes up in interesting ways. That's a ton of innocent people who get sucked into NSA's maw and will continue to even after/if the phone dragnet moves to the providers.

DEA, International

As I said, the analogue to the program described by the USA Today, dubbed USTO, is *not* the Section 215 database, but instead the EO 12333 database (indeed, USAT describes that DEA included entirely foreign metadata in their database as well). The data in this program provided by domestic providers came under 21 USC 876 — basically the drug war equivalent of the Section 215 "tangible things" provision. An DEA declaration in the Shantia Hassanshahi case claims it only provides base metadata, but it doesn't specify whether that includes or excludes location. As USAT describes (and would have to be the case for Hassanshahi to be busted for sanctions violations using it, not to mention FBI's success at stalling of DOJ IG's investigation into it), this database came to be used for other than counternarcotics purposes (note, this should have implications for EO 12333, which I'll get back to). And, as USAT also described, like the NSA dragnet, the USTO also linked right into automatic analysis (and, I'm willing to bet good money, tracked multiple types of metadata). As USAT describes, DEA did far more queries of this database than of the Section 215 dragnet, but that's not analogous; the proper comparison would be with NSA's 12333 dragnet, and I would bet the numbers are at least comparable (if you can even count these automated chaining processes anymore). DEA says this database got shut down in 2013 and claims the data was purged. DEA also likely would like to sell you the Brooklyn Bridge real cheap.

DEA, Domestic

There's also a domestic drug-specific dragnet, Hemisphere, that was first exposed by a NYT article. This is not actually a DEA database at all. Rather, it is a program under the drug czar that makes enhanced telecom data available for drug purposes, while the records appear to stay with the telecom.

This seems to have been evolving since 2007 (which may mark when telecoms stopped turning over domestic call records for a range of purposes). At one point, it pulled off multiple providers' networks, but more recently it has pulled only off AT&T's networks (which I suspect is increasingly what has happened with the Section 215 phone dragnet).

But the very important feature of Hemisphere — particularly as compared to its analogue, the Section 215 dragnet — is that the telecoms perform the same kind of analysis they would do for their own purposes. This includes using location data and matching burner phones (though this is surely one of the automated functions included in NSA's EO 12333 dragnet and DEA's USTO). Thus, by keeping the data at the telecoms, the government appears to be able to do more sophisticated kinds of analysis on domestic data, even if it does so by accessing fewer records.

That is surely the instructive motivation behind Obama's decision to "let" NSA move data back to the telecoms. It'd like to achieve what it can under Hemisphere, but with data from all telecom providers rather than just AT&T.

CIA

At least as the NSA documents concerning ICREACH tell it, CIA and DEA jointly developed a sharing platform called PROTON that surely overlaps with USTO in significant ways. But PROTON appeared to reside with CIA (and FBI and NSA were late additions to the PROTON sharing). PROTON included CIA specific metadata (that is, not

telecommunications metadata but rather metadata tracking their own HUMINT). But in 2006 (these things all started to change around that time), NSA made a bid to become the premiere partner here with ICREACH, supporting more types of metadata and sharing it with international partners.

So we don't know what CIA's own dragnet looks like, just that it has one, one not bound to just telecommunications.

In addition, CIA has a foreign intelligence equivalent of Hemisphere, where it pays AT&T to "voluntarily" hand over data that is at least one-end foreign (and masks the US side unless the record gets referred to FBI).

Finally, CIA can "upload or transfer some or all" of the metadata that it pulls off of raw PRISM data received under 702 into its other databases. While this has to be targeted off a foreign target, that surely includes a lot of US person data, and metadata including Internet based calls, photos, as well as emails. CIA does a lot of metadata queries for other entities (other IC agencies? foreign partners? who knows!), and they don't count it, so they are clearly doing a lot of it.

FBI

As far as we know, FBI does not have a true "bulk" dragnet, sucking up all the phone or Internet records for the US or foreign switches. But it surely has fairly massive metadata repositories itself.

Until 2006, it did, however, have something almost identical to what we understand Hemisphere to be, all the major telecoms, sitting onsite, ready to do sophisticated analysis of numbers offered up on a post-it note, with legal process to follow (maybe) if anything nifty got turned over. Under this program, AT&T offered some bells and whistles, included "communities of interest" that included at least one hop. That all started to get moved

offsite in 2006, when DOJ's IG pointed out that it didn't comply with the law, but all the telecoms originally contracted (AT&T and the companies that now comprise Verizon, at least), remained on contract to provide those services albeit offsite for a few years. In 2009, one of the telecoms (which is likely part or all of Verizon) pulled out, meaning it no longer has a contract to provide records in response to NSLs and other process in the form the FBI pays it to.

FBI also would have a database of the records it has collected using NSLs and subpoenas (I'll go look up the name shortly), going back decades. Plus, FBI, like CIA, can "upload or transfer some or all" of the metadata that it pulls off of raw PRISM data received under 702. So FBI has its own bulky database, but all of the data in it *should* have come in in relatively intentional if not targeted fashion. What FBI does have *should* date back much longer than NSA's Section 215 database (30 years for national security data) and, under the new Section 309 restrictions on EO 12333 data, even NSA's larger dragnet. On top of that, AT&T still provides 7 bells and whistles that are secret and that go beyond a plain language definition of what they should turn over in response to an NSL under ECPA (which probably parallel what we see going on in Hemisphere). In its Section 215 report, PCLOB was quite clear that FBI almost always got the information that could have come out of the Section 215 dragnet via NSLs and its other authorities, so it seems to be doing quite well obtaining what it needs without collecting all the data everywhere, though there are abundant reasons to worry that the control functions in FBI's bulky databases are craptastic compared to what NSA must follow.

“INFORMATION IS NO LONGER BEING COLLECTED IN BULK [PURSUANT TO 21 U.S.C. § 876]”

Given the details in yesterday’s USAT story on DEA’s dragnet, I wanted to re-examine the DEA declaration revealing details of the phone dragnet in the Shantia Hassanshahi case which I wrote about here. As I noted then, there’s a footnote modifying the claim that the database in question “was suspended in September 2013” that is entirely redacted. And the declaration only states that “information is no longer being collected in bulk pursuant to 21 U.S.C. §876,” not that it is no longer being collected.

According to the USAT, DEA moved this collection to more targeted subpoenas that may number in the thousands.

> The DEA asked the Justice Department to restart the surveillance program in December 2013. It withdrew that request when agents came up with a new solution. Every day, the agency assembles a list of the telephone numbers its agents suspect may be tied to drug trafficking. Each day, it sends electronic subpoenas — sometimes listing more than a thousand numbers — to telephone companies seeking logs of international telephone calls linked to those numbers, two official familiar with the program said.
>
> The data collection that results is more targeted but slower and more expensive. Agents said it takes a day or more to pull together communication profiles that used to take minutes.

We should expect this move occurred either in

the second half of 2013 (after the dragnet first got shut down) or the first half of 2014 (after DEA backed off its request to restart the draget). And we should expect these numbers to show in the telecoms transparency reports.

But they don't — or don't appear to.

Both AT&T and Verizon reported their 2013 numbers for the entire year. They both broke out their 2014 numbers semiannually. (Verizon; AT&T 2013; AT&T 2014; h/t Matt Cagle, who first got me looking at these numbers)

Here are the numbers for all subpoenas (see correction below):

	Verizon	**AT&T**
Total 2013	**164,184**	**248,343**
First Half 2014	72,342	86,943
Second Half 2014	65,816	114,811
Total 2014	**138,158**	**201,754**

Both companies show a decrease in overall criminal subpoenas from 2013 to 2014. And while Verizon shows a continued decline, AT&T's subpoena numbers went back up in the second half of 2014, but still lower than half of 2013's numbers.

In any case, both companies report at least 15% fewer subpoenas in 2014, at a time when — according to what USAT got told — they should have been getting thousands of extra subpoenas a day.

It is possible what we're seeing is just the decreased utility of phone records. As the USAT notes, criminals are increasingly using messaging platforms that use the Internet rather than telecoms.

But it's possible the DEA's dragnet went somewhere else entirely.

Though USAT doesn't mention it (comparing instead with the Section 215 dragnet, which is

not a comparable program because it, like Hemisphere as far as we know, focuses solely on domestic records), the NSA has an even bigger phone and Internet dragnet that collects on drug targets. Indeed, President Obama included "transnational criminal threats" among the uses permitted for data collected in bulk under PPD-28, which he issued January 17, 2014. So literally weeks after DEA supposedly moved to subpoena-based collection in December 2013, the President reiterated support for using NSA (or, indeed, any part of the Intelligence Community) bulk collections to pursue transnational crime, of which drug cartels are the most threatening.

There is no technical reason to need to collect this data in the US. Indeed, given the value of location data, the government is better off collecting it overseas to avoid coverage under *US v. Jones*. Moreover, as absolutely crummy as DOJ is about disclosing these kinds of subpoenas, it has disclosed them, whereas it continues to refuse to disclose any collection under EO 12333.

Perhaps it is the case that DEA really replaced its dragnet with targeted collection. Or perhaps it simply moved it under a new shell, EO 12333 collection, where it will remain better hidden.

Update: I realized I had used criminal subpoenas for AT&T, but not for Verizon (which doesn't break out criminal and civil). Moreover, it's not clear whether the telecoms would consider these criminal or civil subpoenas.

I also realized one other possible explanation why these don't show up in the numbers. USAT reports that DEA uses subpoenas including thousands of numbers, whereas they used to use a subpoena to get all the records. That is, the telecoms may count each of these subpoenas as just one subpoena, regardless of whether it obtains 200 million or 1,000 numbers. Which would have truly horrifying implications for "Transparency."

Update: There would be limitations to relying on

the NSA's database (though DEA could create its own for countries of particular interest). First, DEA could not search for US person identifiers without Attorney General approval (though under SPMCA, it could conduct chaining it knew to include US persons). Also, as of August 2014, at least, NSA wasn't sharing raw EO 12333 data with other agencies, per this Charlie Savage story.

> The N.S.A. is also permitted to search the 12333 storehouse using keywords likely to bring up Americans' messages. Such searches must have "foreign intelligence" purposes, so analysts cannot hunt for ordinary criminal activity.
>
> For now, the N.S.A. does not share raw 12333 intercepts with other agencies, like the F.B.I. or the C.I.A., to search for their own purposes. But the administration is drafting new internal guidelines that could permit such sharing, officials said.

That said, it's clear that NSA shares metadata under ICREACH with other agencies, explicitly including DEA.

DEA LIKELY HAS MORE THAN ONE DRAGNET

As yesterday's USAT story on the DEA dragnet reported, DOJ's Inspector General is investigating DEA's dragnet. I first reported that in April 2014.

As I also reported in February, FBI is obstructing that investigation — so much so, that DOJ's Inspector General Michael Horowitz encouraged Congress to start using

appropriations to force it to stop.

> The unfulfilled information request that causes the OIG to make this report was sent to the FBI on November 20,2014. Since that time, the FBI has made a partial production in this matter, and there have been multiple discussions between the OIG and the FBI about this request, resulting in the OIG setting a final deadline for production of all material of February 13,2015.
>
> On February 12, 2015, the FBI informed the OIG that it would not be able to produce the remaining records by the deadline. The FBI gave an estimate of 1-2 weeks to complete the production but did not commit to do so by a date certain. The reason for the FBI's inability to meet the prior deadline set by the OIG for production is the FBI's desire to continue its review of emails requested by the OIG to determine whether they contain any information which the FBI maintains the OIG is not legally entitled to access, such as grand jury, Title III electronic surveillance, and Fair Credit Reporting Act information.

DOJ IG's comments about this investigation are worth reconsideration for two reasons.

First, FBI's obstruction of the investigation emphasize what we already knew from the Shantia Hassanshahi case (via which we first learned about this database). The FBI is (was) also using this database, and for purposes that far exceed counter-narcotics (Hassanshahi was busted for sanctions violations). And, as the Homeland Security investigator's dramatically changing stories about how he first identified Hassanshahi suggest, for each of those usages, there's likely some kind of parallel construction going on.

How many cases have been based off this giant dragnet?

But also look at how DOJ's IG has described this investigation.

> ### *Administrative Subpoenas*
>
> The OIG is examining the DEA's use of administrative subpoenas to obtain broad collections of data or information. The review will address the legal authority for the acquisition or use of these data collections; the existence and effectiveness of any policies and procedural safeguards established with respect to the collection, use, and retention of the data; the creation, dissemination, and usefulness of any products generated from the data; and the use of "parallel construction" or other techniques to protect the confidentiality of these programs.

DOJ IG is investigation DEA's use of subpoenas to obtain *broad collections of data or information*. Its review will address the legal authority underlying *these data collections*.

Collections, plural.

Admittedly, we already know of two DEA dragnets: the international dragnet described by the USAT, and the domestic one — Hemisphere — though that resides at least partially with the White House Drug Czar.

But the authority used in the USAT dragnet, 21 USC 876, is the drug equivalent of Section 215, permitting the agency to obtain "tangible things" relevant to (that phrase again) an investigation. We know FBI used equivalent language under Section 215 to collect financial and Internet records as well.

Hell, the DEA couldn't very well track drug

cartels without following the money, via whatever means. Plus, we know cartels have used things like travelers checks and gift cards to move money in recent years.

So I would be willing to bet more than a few quarters that DOJ IG's use of the term "collections" suggests there's more than just these telecom dragnets hiding somewhere.

EVERYTHING IN THE WAR ON TERROR CAME FROM THE WAR ON DRUGS

bmaz has long insisted, correctly, that all the tricks they have used in the war on terror came first from the war on drugs.

The USA Today's Brad Heath demonstrates how true that is with a blockbuster story on a DEA dragnet, called the USTO, of US to international calls covering up to 116 countries that operated similarly to the NSA dragnet. It dates back to the last days of Poppy Bush's administration. And key figures — especially Robert Mueller, but also Eric Holder — played roles in it in their earlier Executive Branch careers. And, no surprise, the DEA never gave discovery on the collection to defendants.

Definitely read the whole thing. But I'm particularly interested in the last paragraphs, which explain what happened to it. After Snowden exposed the NSA version of the dragnet (which includes the US, as well as foreign countries) and the government kept arguing that was justified because of its special intelligence purpose, the claims they made to justify the DEA dragnet started to fall apart. Plus, it has become less useful anyway, now that more people

use the Intertoobz.

> It was made abundantly clear that they couldn't defend both programs," a former Justice Department official said. Others said Holder's message was more direct. "He said he didn't think we should have that information," a former DEA official said.
>
> By then, agents said USTO was suffering from diminishing returns. More criminals — especially the sophisticated cartel operatives the agency targeted — were communicating on Internet messaging systems that are harder for law enforcement to track.
>
> Still, the shutdown took a toll, officials said. "It has had a major impact on investigations," one former DEA official said.
>
> The DEA asked the Justice Department to restart the surveillance program in December 2013. It withdrew that request when agents came up with a new solution. Every day, the agency assembles a list of the telephone numbers its agents suspect may be tied to drug trafficking. Each day, it sends electronic subpoenas — sometimes listing more than a thousand numbers — to telephone companies seeking logs of international telephone calls linked to those numbers, two official familiar with the program said.
>
> The data collection that results is more targeted but slower and more expensive. Agents said it takes a day or more to pull together communication profiles that used to take minutes.

This lesson is instructive for the NSA dragnet. It points to one reason why the NSA dragnet may not get all the "calls" it wants: because of messaging that bypasses the telecom backbone. And it shows that an alternative approach can be

used.

AMERICAN HEGEMONY: DELIVERING "UNPREDICTABLE INSTABILITY" THE WORLD OVER

I love Global Threat Hearings and curse you Richard Burr for holding the Senate Intelligence Committee's hearing in secret.

At least John McCain had the courage to invite James Clapper for what might have been (but weren't) hard questions in public in front of Senate Armed Services Committee Thursday.

Clapper started with a comment that was not prominent in (though it definitely underscored) his written testimony (Update: Here's the transcript of his as-delivered statement.)

> Unpredictable instability is the new normal.The year 2014 saw the highest rate of political instability since 1992. The most deaths as a result of state-sponsored mass killings since the early 1990s. And the highest number of refugees and internally displaced persons (or IDPs) since World War II. Roughly half of the world's currently stable countries are at some risk of instability over the next two years.

It's a damning catalog. All the more so given that the US has been the world's unquestioned hegemon since that period in the early 1990s

when everything has been getting worse, since that period when the first President Bush promised a thousand points of light.

And while the US can't be held responsible for all the instability in the world right now, it owns a lot of it: serial invasions in the Middle East and the coddling of Israel account for many of the refugees (though there's no telling what would have happened with the hundred thousand killed and millions of refugees in Syria had the second President Bush not invaded Iraq, had he taken Bashar al-Assad up on an offer to partner against al Qaeda, had we managed the aftermath of the Arab Spring differently).

US-backed neoliberalism and austerity — and the underlying bank crisis that provided the excuse for it — has contributed to instability elsewhere, and probably underlies those countries that Clapper thinks might grow unstable in the next year.

We're already seeing instability arising from climate change; the US owns some of the blame for that, and more for squandering its leadership role on foreign adventures rather than pushing a solution to that more urgent problem (Clapper, by the way, thinks climate change is a problem but unlike Obama doesn't consider it the most serious one).

There are, obviously, a lot of other things going on. Clapper talked admiringly of China's modernization of its military, driven by domestically developed programs, an obvious development when a country becomes the manufacturing powerhouse of the world. But China's growing influence comes largely in the wake of, and in part because of, stupid choices the US has made.

There was, predictably, a lot of discussion about cyberthreats, even featuring Senate Intelligence Committee member Angus King arguing we need an offensive threat (we've got one — and have been launching pre-emptive strikes for 9 years now — as he would know if he paid

attention to briefings or read the Intercept or the New York Times) to deter others from attacking us with cyberweapons.

Almost everyone at the hearing wanted to talk about Iran, without realizing that a peace deal with it would finally take a step towards more stability (until our allies the Saudis start getting belligerent as a result).

Still, even in spite of the fact that Clapper started with this inventory of instability, there seemed zero awareness of what a damning indictment that is for the world's hegemon. Before we address all these other problems, shouldn't we focus some analysis on why American hegemony went so badly wrong?

FBI NOW HOLDING UP MICHAEL HOROWITZ' INVESTIGATION INTO THE DEA

Man, at some point Congress is going to have to declare the FBI legally contemptuous and throw them in jail.

They continue to refuse to cooperate with DOJ's Inspector General, as they have been for basically 5 years. But in Michael Horowitz' latest complaint to Congress, he adds a new spin: FBI is not only obstructing his investigation of the FBI's management impaired surveillance, now FBI is obstructing his investigation of DEA's management impaired surveillance.

I first reported on DOJ IG's investigation into DEA's dragnet databases last April. At that point, the only dragnet we knew about was Hemisphere, which DEA uses to obtain years of

phone records as well as location data and other details, before it them parallel constructs that data out of a defendant's reach.

But since then, we've learned of what the government claims to be another database — that used to identify Shantia Hassanshahi in an Iranian sanctions case. After some delay, the government revealed that this was another dragnet, including just international calls. It claims that this database was suspended in September 2013 (around the time Hemisphere became public) and that it is no longer obtaining bulk records for it.

According to the latest installment of Michael Horowitz' complaints about FBI obstruction, he tried to obtain records on the DEA databases on November 20, 2014 (of note, during the period when the government was still refusing to tell even Judge Rudolph Contreras what the database implicating Hassanshahi was). FBI slow-walked production, but promised to provide everything to Horowitz by February 13, 2015. FBI has decided it has to keep reviewing the emails in question to see if there is grand jury, Title III electronic surveillance, and Fair Credit Reporting Act materials, which are the same categories of stuff FBI has refused in the past. So Horowitz is pointing to the language tied to DOJ's appropriations for FY 2015 which (basically) defunded FBI obstruction.

Only FBI continues to obstruct.

There's one more question about this. As noted, this investigation is supposed to be about DEA's databases. We've already seen that FBI uses Hemisphere (when I asked FBI for comment in advance of this February 4, 2014 article on FBI obstinance, Hemisphere was the one thing they refused all comment on). And obviously, FBI access another DEA database to go after Hassanshahi.

So that may be the only reason why Horowitz needs the FBI's cooperation to investigate the DEA's dragnets.

Plus, assuming FBI is parallel constructing these dragnets just like DEA is, I can understand why they'd want to withhold grand jury information, which would make that clear.

Still, I can't help but wonder — as I have in the past — whether these dragnets are all connected, a constantly moving shell game.

That might explain why FBI is so intent on obstructing Horowitz again.