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?