

THE KIDDIE PORN AND THE UNDIEBOMB

I was
at a
funera
l
Monday
and
Tuesda
y. So
when I



heard the FBI had busted the guy who leaked the UndieBomb 2.0 story, I assumed they had finally arrested John Brennan.

But, as bmaz emphasized in his post on Donald Sachtleben's plea agreement, there's no hint of prosecuting Brennan, who leaked Top Secret details about the British/Saudi double agent into AQAP, even while they're imprisoning Donald Sachtleben, who is only accused of leaking details he knew to be Secret.

A law enforcement official indicated that the case has not been officially closed but the charges against Sachtleben are the only ones expected.

(Sure, the evidence that Sachtleben was involved with kiddie porn seems solid, but then Brennan drone-killed children, so he's not above reproach for his treatment of children either.)

But that is by no means the weirdest thing about the government's treatment of the UndieBomb 2.0 leak investigation.

The entire premise of the FBI narrative is that they exercised greater care with a kiddie porn accusee they had dead to rights than they did the 100 or so AP reporters who got sucked up in their overbroad dragnet. They would have you believe that, even after seizing a CD holding a November 2, 2006 SECRET CIA intelligence report at Sachtleben's house in May 2012 pursuant to a

kiddie porn warrant (which they have not produced in the docket), they just sat on his devices for almost a year until they obtained the phone records for 20 AP phone lines, in a seizure far more intrusive into journalism than any recent known subpoena.

Sachtleben was identified as a suspect in the case of this unauthorized disclosure only after toll records for phone numbers related to the reporter were obtained through a subpoena and compared to other evidence collected during the leak investigation. This allowed investigators to obtain a search warrant authorizing a more exhaustive search of Sachtleben's cell phone, computer, and other electronic media, which were in the possession of federal investigators due to the child pornography investigation.

(I may be mistaken, but I don't think the FBI made this claim in any court document, so I assume it is bullshit, especially since they had had to do extensive forensic searches of Sachtleben's computer and he had already signed a plea deal forfeiting it.)

They would also have you believe the AP had no inkling of the UndieBomb plot until ABC reported inflammatory claims about cavity bombs on April 30, 2012, even in spite of ABC's reference to TSA head John Pistole's earlier fear-mongering about it and in spite of additional reporting about broad Air Marshall mobilization. DOJ goes to great lengths to make you believe AP first texted Sachtleben on April 30 and not, say, on April 28 (which would mean the kiddie porn investigation accelerated after such contact), though there's no reason to believe that's true and the AP call records DOJ obtained apparently go back to well before April 30. They also suggest AP was asking Sachtleben about an Asiri bomb, though the first text they include is an assertion – not a question – that Asiri has been busy.

They would have you believe that two Pulitzer Prize winners would defy White House and CIA wishes with a story sourced to a single source who, just a day earlier, had provided a mistaken guess about the excitement. They would have you believe that Adam Goldman (probably) would be added as a byline to a Matt Apuzzo story for shits and giggles, not for reporting beyond the few text messages and 2-minute phone call they depict Apuzzo (probably) as having had. In short, they would have you believe they caught the single solitary guy behind this story (though if it were true it'd make it all the more clear that the real damage was done by Brennan and not Sachtleben), even while the AP story makes it clear there were multiple sources, some discussing topics not depicted in the FBI's account.

They would also have you believe that they arrested Sachtleben (after tailing him in the airport) for what they claim they had evidence to be a small collection of kiddie porn the minute they executed a search of his house and did an initial triage of his computer (they would ultimately find more), but let Jason Nicoson, the guy through whom they claim to have found Sachtleben, a guy they believed to have far more porn, wander free for 8 more months (though Nicoson's magistrate docket appears to be sealed so there may be an earlier arrest).

And they would have you believe that they would arrest a guy who had been working in the immediate vicinity of the UndieBomb in between the time the government learned of the imminent story and its publication, seize his devices, as well as a SECRET November 2, 2006 CIA intelligence report, but that that arrest had nothing to do with **nor led to** suspicions he was also the leaker.

It's an interesting tale, but so much of it doesn't make sense no one should believe it.

Which is not to say I know what happened. It could be it happened just like they said it did, but it looks so weird because the embarrassment

of having an ex-FBIer caught with kiddie porn made every one squeamish. It could be the FBI already knew about Sachtleben's proclivities (perhaps back to the September 2011 noted in their narrative), but only decided to bust him when they realized he was leaking to journalists (and there's no reason to assume he talked just to the AP). It could be the FBI loaded up the porn when he was in Quantico – after all **he had his laptop with him** (!!) on that trip (who brings a laptop full of kiddie porn into Quantico or anywhere close?). It could be they discovered Sachtleben was a minor source for the story because of things they found as part of the May 11 search – but not the source tying the operation more closely to Fahd al-Quso – but didn't bust him for it until they decided he would be the one and only (public) scapegoat for the story.

But the seizure of that CIA report and the placement of Sachtleben in the UndieBomb examination room and the ability to get Sachtleben's contact records without a warrant would have provided the FBI reasonable suspicion to get a warrant to search the rest of his devices long before DOJ seized AP's phone records. Had they wanted to investigate Sachtleben for his potential role in leaking to the AP in 2012, they had the means to do so.

Which seems to indicate two things. This story is meant to provide closure to the leak investigation the GOP demanded as well as a public excuse for seizing 100 journalists' metadata they didn't need to find the ultimate sole public culprit. (It helps, too, that DC US Attorney Ronald Machen was able to shunt this matter off to Indiana, so DC reporters couldn't look for any sealed underlying dockets in DC.)

When DOJ released its "new" reporters guidelines, they made it clear they intended to deal with leakers internally now.

The Department will work with others in the Administration to explore ways in which the intelligence agencies

themselves, in the first instance, can address leaks internally through administrative means, such as the withdrawal of security clearances and the imposition of other sanctions.

Intelligence Community Inspector General Charles McCullough was already working on hundreds of such investigations going back to November 2011 (see also this post). It's likely we're already seeing the new mode of dealing with leaks – at least for favored sources leaking to favored reporters – in the stripping of James Cartwright's security clearance.

But DOJ has long had it in for Apuzzo and Goldman. DOJ twice before investigated their sources (for this story and this one). And with Sachtleben, they had the means to conduct a breathtaking seizure of AP call records (making those internal investigations into AP's other sources far easier), with a means to tie the most rudimentary part of this leak to a sleazy kiddie porn prosecution.

A timeline of these two purportedly parallel investigations is below. You tell me whether FBI's claims don't seem ridiculous?

1993: Sachtleben works on aftermath of first World Trade Center bombing

1998: Sachtleben works on aftermath of African Embassy bombings

2000: Sachtleben works on aftermath of Cole bombing

2001: Sachtleben works on aftermath of 9/11 attack

November 2, 2006: Date of CIA intelligence report specifically charged

2008: Sachtleben retires from FBI, begins contracting on same or closely related work

Fall 2009: Sachtleben starts serving as source

for Matt Apuzzo or Adam Goldman (probably the former, as he was already covering DOJ)

January 2010: Sachtleben provides AP information on terrorist plots, presumably (especially given text referring to Ibrahim al-Asiri) UndieBomb 1.0

September 12, 2010: Special Agent finds images tied to pedodad36569 (AKA Jason Nicoson)

September 2011: Paragraph 29 of Kiddie Porn charges dates back to September 2011—why? New laptop?

October 7, 2011: Obama orders Insider Threat Detection program

October 25, 2011: pedodave69 (AKA Sachtleben) emails pedodad36569 offering to share porn; this is FBI's explanation for the investigation into Sachtleben

December 27, 2011: Sprint identifies pedodad36569 as Jason Nicoson

Undated: FBI searches Nicoson's email account, finds October 25, 2011 email from pedodave69 [I've placed this in different position than government because something must have justified the Nicoson warrant and there must be some reason DOJ doesn't give this date – it may well be even earlier]

January 9, 2012: FBI searches Nicoson's house; he admits to trading kiddie porn

February 20, 2012: Last use of pedodave69 email "observed"

March 29, 2012: FBI serves administrative subpoena on AT&T for pedodave69's IP

April 1, 2012: Possible start date for seizure of AP records

April 11, 2012: AT&T informs FBI pedodave69's IP belongs to Donald Sachtleben

Around April 20, 2012: UndieBomb recovered

April 24, 2012: Robert Mueller reportedly in

Yemen

April 30, 2012: FBI conducts wireless survey of Sachtleben's vicinity and finds his secure wireless; an NCIC search comes back negative, an open source check reveals Sachtleben lives there, **search of "law enforcement sensitive database" reveals he lives there**

April 30, 2012, 6:30PM: ABC reports on cavity bombs

April 30, 2012, 7:14PM: AP journo and Sachtleben started texting. [Note, the statement of offense says they got this from Sachtleben's devices.]

AP: Al-Asiri is up to his old tricks. I wonder if ur boys got a hold of a cavity bomb. :)

Sachtleben: Yikes. Remind me to bring sum purell to the lab

AP: Not totally sure though

May 1, 2012, AM: AP journo and Sachtleben continue texting.

Sachtleben: Hmm. Methinks the 10am news conf may be related. 9:48AM

AP: Ah! 9:51AM

Sachtleben: Just abt to take off. Will be curious to c coverage when I land at dulles. Hope that tsa doesnt get out the rubber gloves and ky 9:52AM

May 1, 2012: **Search of (apparently) same law enforcement sensitive database** reconfirms Sachtleben lives there (?)

May 1, 2012, 10:00AM: At press conference, FBI announces arrest of 5 Occupy-tied activists in bombing plot

May 1, 2012, 12:49PM: Sachtleben corrects his earlier guess.

Sachtleben: Got that one wrong. A lil

surprised they r wrkin 24 hr shifts cuz
of those mutts. **Still mght b sumthin
else brewin. Will find out
tomorrow** [emphasis FBI's]

May 2, 2012, 8:39AM: Sachtleben goes to work at Quantico. He's working in Explosives Unit, which is where they are investigating the UndieBomb. He accesses the room where they are investigating it (the documents don't say whether he was supposed to be working on it, though given his earlier probable work on UndieBomb 1.0 you'd think he'd at least be consulted).

May 2, 2012, 10:25AM: Sachtleben calls AP, speaks for 2 minutes. Discloses information he believes to be at least Secret and presumably involves the CIA.

FBI was then engaged in an ongoing, secretive, and sensitive analysis of the bomb; analysis which involved other parts of the United States government besides the FBI.

May 2, 2012, approximately 1PM: AP calls "multiple United States Government officials" and stated,

1. US had intercepted a bomb from Yemen
2. FBI was analyzing the bomb
3. They believed AQAP's bombmaker Ibrahim al-Asiri linked to bomb

Government asks AP to delay reporting UndieBomb 2.0 story.

May 2, 2012: FBI claims to conduct physical surveillance of Sachtleben's house and sees same red pickup viewed in Google view (see above; h/t William Ockham)

May 3, 2012: FBI obtains search warrant (it

doesn't appear in Sachtleben's docket)

May 6, 2012: Fahd al-Quso killed

May 7, 2012: Government tells AP national security concerns have been allayed; AP publishes story including the following additional details:

- The bomb was an upgraded design from UndieBomb 1.0 (sourced to "US officials") that did not contain metal and might not be IDed by Rapiscan machines
- The bomber had not yet picked a flight (this has always suggested that the AP did not yet know the plot was a Saudi-sting)
- White House and DHS officials said they knew of no Osama bin Laden raid anniversary attacks (see this post)
- AP learned about plot "last week" but held off on request from White House and CIA; concerns now allayed
- Details from Caitlin Hayden statement
- "Authorities" suspect al-Asiri made the bomb
- Fahd al-Quso killed

Note, several of these details are not specifically sourced; the anonymous ones that are are sourced to "US government officials" and "authorities"—both plural.

May 7, 2012: John Brennan briefs former CT Czars, indicates we had inside source, which

leads to disclosure of British/Saudi infiltrator

May 8, 2012: ABC reveals UndieBomb inside job

May 10, 2012: Peter King calls for investigation of AP's (but not ABC's) sources (he also claims Speaker Boehner hadn't been briefed and "very few in the FBI" knew about it)

May 11, 2012: Sachtleben returns to Indianapolis from Quantico; FBI Special Agents observed him carrying a laptop as he arrived at the airport, suggesting they were tailing him already; he drives his Chevy Suburban (not the red truck in the Google surveillance) from the airport; FBI and local law enforcement execute the May 3 search warrant as he arrives; FBI did a "limited on scene triage" of the computer and found images tying him to pedodad36569; Sachtleben's contract with FBI terminated; (presumably same date) FBI also seizes November 2, 2006 SECRET/NOFORN CIA intelligence report charged in leak case

May 7 to May 15, 2012 (presumably): Sachtleben continues to provide AP information on UndieBomb

May 15, 2012: CBS reports Sachtleben's Kiddie Porn arrest

May 17, 2012: At bail hearing, government introduces two sealed exhibits supporting continued detention, but magistrate releases Sachtleben on bail

May 21, 2012: Peter King formally asks Robert Mueller to investigate UndieBomb 2.0

May 23, 2012: Patrick Fitzgerald resigns (Nicoson investigation was in NDIL, western district)

June 11, 2012: Government files for extension on indictment with Sachtleben agreement

July 19, 2012: DOD rolls out Insider Threat program

August 7, 2012: Jason Nicoson indicted

August 10, 2012: Information in lieu of

indictment

September 5, 2012: Status hearing

October 1, 2012: Continuance of trial

November 7, 2012: Motion to change plea, extend time, anticipating plea by December

Around February 9, 2013: DOJ obtains AP records

April 3, 2013: Status hearing set for April 23

April 18, 2013: Status hearing vacated

May 10, 2013: Ronald Machen informs AP it took 20 phone lines worth of call records; the seizure was probably 90 days earlier

May 13, 2013: Plea agreement on kiddie porn; AP reveals DOJ phone record seizure

May 20, 2013: Jason Nicoson plea agreement

July 7, 2013: Because of his attorney's scheduling conflict, Sachtleben asks to continue plea and sentencing to August 13

July 9, 2013: Sachtleben stops possessing classified documents at his house (no search warrant described)

Between August 7 and 28, 2013: Government submits two motions (one is for revocation of pretrial release) that are sealed on August 28

August 30, 2013: In hearing, government argues for change of conditions of release; filed under separate (now sealed) order

September 4, 2013: Superseding plea agreement on kiddie porn also requires guilty plea on leak

September 23, 2013: Leak plea agreement