TWO DAYS AFTER JULIAN ASSANGE THREATENED DON JR, ACCUSED VAULT 7 LEAKER JOSHUA SCHULTE TOOK TO TOR

Monday, the government rolled out a superseding indictment for former NSA and CIA hacker Joshua Schulte, accusing him (obliquely) of leaking the CIA's hacking tools that became the Vault 7 release from Wikileaks. The filings in his docket (as would the search warrants his series of defense attorneys would have seen) make it clear that the investigation into him, launched just days after the first CIA release, was always about the CIA leak. But when the government took his computer last spring, they found thousands of child porn pictures dating back to 2009. It took the government over three months and a sexual assault indictment in VA to convince a judge to revoke his bail last December, and then another six months to solidify the leaking charges they had been investigating him from the start.

But the case appears to have taken a key turn on November 16, 2017, when he did something — it's not clear what — on the Tor network. While there are several things that might explain why he chose to put his release at risk by accessing Tor that day, it's notable that it occurred two days after Julian Assange tweeted publicly to Donald Trump Jr that he'd still be happy to be Australian Ambassador to the US, implicitly threatening to release more CIA hacking tools.

Schulte was, from days after the initial Vault 7 release, apparently the prime suspect to be the leaker. As such, the government was *always* interested in what Schulte was doing on Tor. In response to a warrant to Google served in March

2017, the government found him searching, on May 8, 2016, for how to set up a Tor bridge (Schulte has been justifiably mocked for truly abysmal OpSec, and Googling how to set up a bridge is one example). That was right in the middle of the time he was deleting logs from his CIA computer to hide what he was doing on it.

When he was granted bail, he was prohibited from accessing computers. But because the government had arrested him on child porn charges and remained coy (in spite of serial hold-ups with his attorneys regarding clearance to see the small number of classified files the government found on his computer) about the Vault 7 interest, the discussions of how skilled he was with a computer remained fairly oblique. But in their finally successful motion to revoke Schulte's bail, the government revealed that Schulte had not only accessed his email (via his roommate, Schulte's lawyer would later claim), but had accessed Tor five times in the previous month, on November 16, 17, 26, and 30, and on December 5, 2017, which appears to be when the government nudged Virginia to get NYPD to arrest him on a sexual assault charge tied to raping a passed out acquaintance at his home in VA in 2015.

Perhaps the most obvious explanation for why Schulte accessed Tor starting on November 16, 2017, is that he was trying to learn about the assault charges filed in VA the day before.

But there is a more interesting explanation.

As you recall, back in November 2017, some outlets began to publish a bunch of previously undisclosed DMs between Don Jr and Wikileaks. Most attention focused on Wikileaks providing Don Jr access to an anti-Trump site during the election. But I was most interested in Julian Assange's December 16, 2016 "offer" to be Australian Ambassador to the US — basically a request for payback for his help getting Trump elected.

> Hi Don. Hope you're doing well! In

> relation to Mr. Assange: Obama/Clinton placed pressure on Sweden, UK and Australia (his home country) to illicitly go after Mr. Assange. It would be real easy and helpful for your dad to suggest that Australia appoint Assange ambassador to DC “That’s a really smart tough guy and the most famous australian you have! ” or something similar. They won’t do it, but it will send the right signals to Australia, UK + Sweden to start following the law and stop bending it to ingratiate themselves with the Clintons. 12/16/16 12:38PM

In the wake of the releases, on November 14, 2017, Assange tweeted out a follow-up.

As I noted at the time, the offer included an implicit threat: by referencing “Vault 8,” the name Wikileaks had given to its sole release, on November 9, 2017 of an actual CIA exploit (as opposed to the documentation that Wikileaks had previously released), Assange was threatening to dump more hacking tools, as Shadow Brokers had done before it. Not long after, Ecuador gave Assange its first warning to stop meddling in other countries politics, explicitly pointing to his involvement in the Catalan referendum but also pointing to his tampering with other countries. That warning became an initial ban on visitors and Internet access in March of this year followed by a more formal one on May 10, 2018 that remains in place.

There's a reason I think those Tor accesses may actually be tied to Assange's implicit threat. In January of this year, when his then lawyer Jacob Kaplan made a bid to renew bail, he offered an excuse for those Tor accesses. He claimed Schulte was using Tor to research the diaries on his experience in the criminal justice system.

> In this case, the reason why TOR was accessed was because Mr. Schulte is writing articles, conducting research and writing articles about the criminal justice system and what he has been through, and he does not want the government looking over his shoulder and seeing what exactly he is searching.

Someone posted those diaries to a Facebook account titled "John Galt's Defense Fund" on April 20, 2018 (in addition to being an accused rapist and child porn fan, Schulte's public postings show him to be an anti-Obama racist and an Ayn Rand worshiping libertarian).

Yesterday, Wikileaks linked those diaries, which strikes me as an attempt to corroborate the alibi Schulte has offered for his access to Tor last November.

The government seems to have let Schulte remain free for much of 2017, perhaps in search of

evidence to implicate him in the Vault 7 release. Whether it was a response to a second indictment or to Assange's implicit threats to Don Jr, Schulte's use of Tor last year (and, surely, the testimony of the roommate he was using as a go-between) may have been one of the keys to getting the proof the government had been searching for since March 2017.

Whatever it is, both Wikileaks and Schulte would like you to believe he did nothing more nefarious than research due process websites when he put his bail at risk by accessing Tor last year. I find that a dubious claim.

2009: IRC discussions of child porn

2011 and 2012: Google searches for child porn

April 2015: Rapes a woman (possibly partner) who is passed out and takes pictures of it

March to June 2016: Schulte deleting logs of access to CIA computer

May 8, 2016: Schulte Googles how to set up a Tor bridge

November 2016: Leaves CIA, moves to NY, works for Bloomberg

December 16, 2016: Assange DM to Don Jr about becoming Ambassador

> Hi Don. Hope you're doing well! In relation to Mr. Assange: Obama/Clinton placed pressure on Sweden, UK and Australia (his home country) to illicitly go after Mr. Assange. It would be real easy and helpful for your dad to suggest that Australia appoint Assange ambassador to DC "That's a really smart tough guy and the most famous australian you have! " or something similar. They won't do it, but it will send the right signals to Australia, UK + Sweden to start following the law and stop bending it to ingratiate themselves with the

> Clintons. 12/16/16 12:38PM

February 4, 2017: Wikileaks starts prepping Vault 7

March 7, 2017: Wikileaks starts releasing Vault 7

March 13, 2017: Google search warrant

March 20, 2017: Search (including of cell phone, from which passwords to his desktop obtained)

June 2017: Interview

August 17, 2017: Dana Rohrabacher tries to broker deal for Assange with Trump

August 23, 2017: Arrest affidavit

August 24, 2017: Arraignment

> THE COURT: Well, it sounds like, based on the interview, that he knew what the government was looking at.
>
> MR. LAROCHE: That wasn't the basis of the interview, your Honor.

> MR. KOSS: I think it was either two or three [interviews]. I think it was three occasions. I was there on all three, including one of which where we handed over the telephone and unblocked the password to the phone, which they did not have, and gave that to them. And as I said, I have been in constant contact with the three assistant U.S. attorneys working on this matter literally on a weekly basis for the last 4, 5, 6 months. And any time Mr. Schulte even thought about traveling, I provided them an itinerary. I cleared it with them first and made sure it was okay. On any occasion that they said they might want him close so that he could speak to them, I cancelled the travel and

> rescheduled it so that we would be available if they needed him at any given time.

September 13, 2017: Bail hearing

> MR. LAROCHE: Well, I believe there still is a danger because it's not just computers, your Honor, but electronic devices are all over society and easy to procure and this type of defendant having the type of knowledge he has does in terms of accessing things – so he has expertise and not only just generally computers but using things such as wiping tools that would allow him to access certain website and leave no trace of it. Those can be done from not just a computer but from other electronic devices.
>
> But the child pornography itself is located on the defendant's desktop computer. They can be accessed irrespective of those servers. So if all the government had was this desktop computer, we could recover the child pornography. So I think this idea that numerous people had access to the serves and potentially could have put it there, is simply a red herring. This was on the defendant's desktop computer. And the location where it was found, this sub-folder within several layers of encryption, there were other personal information of the defendant in that area. There was his bank accounts. I think there was even a resume for the defendant where he was storing this information. And the passwords that were used to get into that location, those passwords were the same passwords the defendant used to access his bank account, to access various other accounts that are related to him. So this idea that he shared them with other people, the government just strongly

> disagrees.

October 11, 2017: Schulte lawyer Spiro withdraws

October 24, 2017: At Trump's request Bill Binney meets with Mike Pompeo to offer alternate theory of the DNC hack

November 8, 2017: Status hearing

> SMITH: I believe the government has told us that there's more data in this case than in any other like case that they have prosecuted.
>
> MR. STANSBURY: Let me just clarify that part first. We proposed this just in an abundance of caution given the defendant's former employer and the fact that — and I meant to flag this before. I apologize now for not. There's a small body of documents that were found in the defendant's residence that were taken from his former employer that might implicate some classified issues. We have been in the process of having those reviewed and I think we're going to be in a position to produce those in the next probably few days. But we wanted to just make sure that we were acting out of an abundance of caution in case any SEPA [sic] issues come about in the case. I don't expect them too at this point but we wanted to do that out of an abundance of caution.

November 9, 2017: Wikileaks publishes Vault 8 exploit

November 14, 2017: Assange posts Vault 8 Ambassador follow-up

November 14, 2017: Arrest warrant in VA

November 15, 2017: Charged in Loudon County for sexual assault

November 16, 2017: Use of Tor

November 17, 2017: Use of Tor

November 26, 2017: Use of Tor

November 29, 2017: Abundance of caution, attorney should obtain clearance

November 30, 2017: Use of Tor

December 5, 2017: Use of Tor, Smith withdraws

December 7, 2017: NYPD arrests on VA warrant for sexual assault

December 12, 2017: Move for detention, including description of email and Tor access

> Separately, since the defendant was released on bail, the Government has obtained evidence that he has been using the Internet. First, the Government has obtained data from the service provider for the defendant's email account (the "Schulte Email Account"), which shows that the account has regularly been logged into and out of since the defendant was released on bail, most recently on the evening of December 6, 2017. Notably, the IP address used to access the Schulte Email Account is

> almost always the same IP address associated with the broadband internet account for the defendant's apartment (the "Broadband Account")—i.e., the account used by Schulte in the apartment to access the Internet via a Wi-Fi network. Moreover, data from the Broadband Account shows that on November 16, 2017, the Broadband Account was used to access the "TOR" network, that is, a network that allows for anonymous communications on the Internet via a worldwide network of linked computer servers, and multiple layers of data encryption. The Broadband Account shows that additional TOR connections were made again on November 17, 26, 30, and December 5.
>
> [snip]
>
> First, there is clear and convincing evidence that the defendant has violated a release condition—namely, the condition that he shall not use the Internet without express authorization from Pretrial Services to do so. As explained above, data obtained from the Schulte Email Account and the Broadband Account strongly suggests that the defendant has been using the Internet since shortly after his release on bail. Especially troubling is the defendant's apparent use on five occasions of the TOR network. TOR networks enable anonymous communications over the Internet and could be used to download or view child pornography without detection. Indeed, the defendant has a history of using TOR networks. The defendant's Google searches obtained in this investigation show that on May 8, 2016, the defendant conducted multiple searches related to the use of TOR to anonymously transfer encrypted data on the Internet. In particular, the defendant had searched for "setup for

> relay," "test bridge relay," and "tor relay vs bridge." Each of these searches returned information regarding the use of interconnected computers on TOR to convey information, or the use of a computer to serve as the gateway (or bridge) into the TOR network.

December 14, 2017: US custody in NY

> MR. KAPLAN: Well, your Honor, we've obtained the discovery given to prior counsel, and I've started to go through that. In addition, there was one other issue which I believe was raised at our prior conference, which was a security clearance for counsel to go through some of the national security evidence that might be present in the case.
>
> While most of the national security stuff does not involve the charges, the actual charges against Mr. Schulte, the basis for the search warrants in this case involve national security.
>
> So I'm starting the process with their office to hopefully get clearance to go through some of the information on that with an eye towards possibly a Franks motion going forward. So I would ask for more time just to get that rolling.

January 8, 2018: Bail appeal hearing

> MR. KAPLAN: Judge, on the last court date, when we left, the idea was that we had consented to detention with the understanding that Mr. Schulte would be sent down to Virginia to face charges based on a Virginia warrant. None of that happened. Virginia never came to get him. Virginia just didn't do anything in this case. But before I address the bail issues, I think it's important that this Court hear the full story of how we actually get here. At

one of the previous court appearances, I believe it was the November 8th date, this Court asked why the defense attorney in this case would need security clearance. And the answer that was given by one of the prosecutors, I believe, was that there was some top secret government information that was found in Mr. Schulte's apartment, and that out of an abundance of caution it would be prudent that the defense attorney get clearance. But I don't think that's entirely accurate.

While the current indictment charges Mr. Schulte with child pornography, this case comes out of a much broader perspective. In March of 2017, there was the WikiLeaks leak, where 8,000 CIA documents were leaked on the Internet. The FBI believed that Mr. Schulte was involved in that leak. As part of their investigation, they obtained numerous search warrants for Mr. Schulte's phone, for his computers, and other items, in order to establish the connection between Mr. Schulte and the WikiLeaks leak.

As we will discuss later in motion practice, we believe that many of the facts relied on to get the search warrants were just flat inaccurate and not true, and part of our belief is because later on, in the third or fourth search warrant applications, they said some of the facts that we mentioned earlier were not accurate. So we will address this in a Franks motion going forward, but what I think is important for the Court is, in April or May of 2017, the government had full access to his computers and his phone, and they found the child pornography in this case, but what they didn't find was any connection to the WikiLeaks investigation. Since that point, from

> May going forward, although they later argued he was a danger to the community, they let him out; they let him travel. There was no concern at all. That changed when they arrested him in August on the child pornography case.
>
> [snip]
>
> The second basis that the government had in its letter for detaining Mr. Schulte was the usage of computers. In the government's letter, they note how, if you search the IP address for Mr. Schulte's apartment, they found numerous log-ons to his Gmail account, in clear violation of this court's order. But what the government's letter doesn't mention is that Mr. Schulte had a roommate, his cousin, Shane Presnall, and this roommate, who the government and pretrial services knew about, was allowed to have a computer.
>
> And more than that, based on numerous conversations, at least two conversations between pretrial services, John Moscato, Josh Schulte and Shane Presnall, it was Shane's understanding that pretrial services allowed him to check Mr. Schulte's e-mail and to do searches for him on the Internet, with the idea that Josh Schulte himself would not have access to the computer.
>
> And the government gave 14 pages of log-on information to establish this point. And, Judge, we have gone through all 14 pages, and every single access and log-in corresponds to a time that Shane Presnall is in the apartment. His computer has facial recognition, it has an alphanumeric code, and there is no point when Josh Schulte is left himself with the computer without Shane being there, and that was their understanding.
>
> LAROCHE: And part of that investigation

is analyzing whether and to what extent TOR was used in transmitting classified information. So the fact that the defendant is now, while on pretrial release, using TOR from his apartment, when he was explicitly told not to use the Internet, is extremely troubling and suggests that he did willfully violate his bail conditions.

KAPLAN: In this case, the reason why TOR was accessed was because Mr. Schulte is writing articles, conducting research and writing articles about the criminal justice system and what he has been through, and he does not want the government looking over his shoulder and seeing what exactly he is searching.

LAROCHE: Because there is a classified document that is located on the defendant's computer, it is extremely difficult, and we have determined not possible, to remove that document forensically and still provide an accurate copy of the desktop computer to the defendant.

So in those circumstances, defense counsel is going to require a top secret clearance in order to view these materials. It's my understanding that that process is ongoing, and we have asked them to expedite it. As soon as the defendant's application is in, we believe he will get an interim classification to review this material within approximately two to three weeks. Unfortunately, that hasn't occurred yet. So the defendant still does not have access to that particular aspect of discovery. So we are working through that as quickly as we can.

January 17, 2018: Bail appeal denied

March 15, 2018: Sabrina Shroff appointed

March 28, 2018: Initial ban of Internet access and visitors for Assange

April 20, 2018: Schulte's diaries (ostensibly the purpose of using Tor) posted

May 10, 2018: Ecuador bans visitors for Assange

May 16, 18, 2018: Documents placed in vault

May 16, 2018: Schulte Facebook site starts legal defense fund

June 18, 2018: Schulte superseding indictment

June 19, 2018: Wikileaks posts links to diary