ON JOSH SCHULTE'S CONTINUED ATTEMPTS TO HACK THE JUDICIAL SYSTEM

Last June, I argued that accused Vault 7 leaker Josh Schulte's decision to represent himself involved a plan to "hack" the judicial system, not with computer code, but by introducing commands into the legal system to make it malfunction.

> Joshua Schulte attempted to complete a hack of the court system yesterday.
>
> I don't mean that Schulte used computer code to bring down the court systems. His laptop doesn't connect to the Internet, and so he does not have those tools available. Rather, over the 3.5 years he has been in jail, he has tested the system, figured out which messages can be used to distract adversaries, and which messages have an effect that will lead the system to perform in unexpected ways. He identified vulnerabilities and opportunities — SDNY arrogance, the pandemic and related court delays, Louis DeJoy's postal system, and even the SAMs imposed on him — and attempted to exploit them.
>
> [snip]
>
> It is almost without exception an insanely bad idea for a defendant to represent themselves, and this is probably not that exception. Still, there are advantages that Schulte would get by representing himself. He's brilliant, and clearly has been studying the law in the 3.5 years he has been in prison (though he has made multiple errors of process and judgment in his own filings). He has repeatedly raised

> the Sixth Amendment problems with Special Administrative Measures, notably describing how delays in receiving his mail make it impossible for him to respond to legal developments in timely fashion. So I imagine he'd prepare a Sixth Amendment challenge to everything going forward. He'd be able to demand access to the image of the server he is alleged to have hacked himself. By proceeding pro se, Schulte could continue to post inflammatory claims to the docket for sympathetic readers to magnify, as happened with a filing he submitted earlier this year. And after the government has made clear it will reverse its disastrous strategy from the first trial of making the trial all about Schulte's conflicts with the CIA, by questioning witnesses himself, Schulte would be able to make personality conflicts central again, even against the government's wishes. Plus, by not replacing Bellovin, Schulte would serve as expert himself. In that role, Schulte would present the false counter story he has been telling since he was jailed, but in a way that the government couldn't cross-examine him. So it would probably be insanely detrimental, but less so than for most defendants that try it. It certainly would provide a way to mount the defense that Schulte clearly wants to pursue.

I also noted the signs that what Schulte really wanted to do was act as co-counsel with his attorneys, something prohibited by precedent in the 2nd Circuit.

Much of this has held up (though not regarding Steve Bellovin, Schulte's superb expert; Schulte has effectively just waited for Bellovin to become available again). Schulte has engaged in the legal equivalent of a DDOS attack, with dozens of motions in the last year, many serial

repeats of the same arguments rejected already, and seventeen appeals of one sort or another.

It appears that Schulte may still be attempting to have hybrid counsel. In a New Yorker profile that came out this week, his attorney, Sabrina Shroff, described how by going pro se, Schulte will not be bound by the legal ethics she is (particularly if he's willing to face further charges for whatever he does at trial — his potential sentence is already so long any additional contempt or leaking charges might make little difference).

> When you consider the powerful forces arrayed against him—and the balance of probabilities that he is guilty—Schulte's decision to represent himself seems reckless. But, for the C.I.A. and the Justice Department, he remains a formidable adversary, because he is bent on destroying them, he has little to lose, and his head is full of classified information. "Lawyers are bound," Shroff told me. "There are certain things we can't argue, certain arguments we can't make. But if you're *pro se* "—representing yourself—"you can make all the motions you want. You can really try your case."

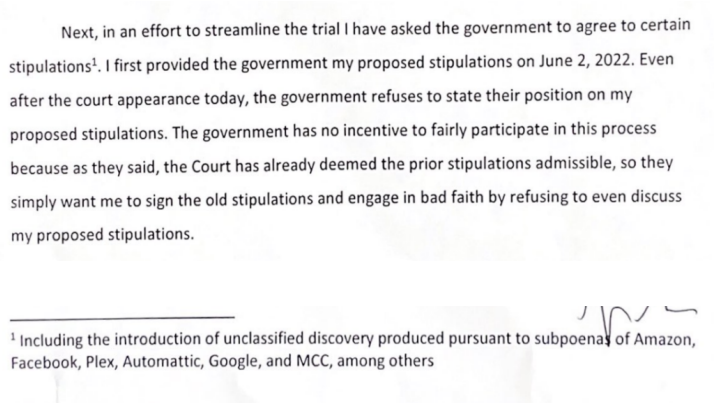
Nevertheless, Schulte recently wrote a letter inquiring about whether Shroff could cross-examine some of the witnesses and issue objections for him.

I fully expect Schulte to make his contentious relationship with his colleagues a central feature of the trial (Schulte even attempted, unsuccessfully, to exclude the one CIA witness who remained on good terms with him, which would have made it easy to portray his targeting as a vendetta by colleagues who hate him). I expect Schulte to disclose information about his colleagues — perhaps including that Jeremy Weber, a pseudonym, appears under his real name in the Ashley Madison hack, an allegation

Schulte seemed primed to make in 2018. Whatever else Schulte does, he will attempt to raise the costs of this trial on the CIA.

Stipulating stipulations

No doubt he has other stunts planned. Schulte claimed this week that the government is refusing to stipulate to things from official custodians (like Google).



Next, in an effort to streamline the trial I have asked the government to agree to certain stipulations[1]. I first provided the government my proposed stipulations on June 2, 2022. Even after the court appearance today, the government refuses to state their position on my proposed stipulations. The government has no incentive to fairly participate in this process because as they said, the Court has already deemed the prior stipulations admissible, so they simply want me to sign the old stipulations and engage in bad faith by refusing to even discuss my proposed stipulations.

[1] Including the introduction of unclassified discovery produced pursuant to subpoenas of Amazon, Facebook, Plex, Automattic, Google, and MCC, among others

This doesn't make sense, unless Schulte is trying to undermine the regularity of this evidence with stipulations.

All that said, I think I may have underestimated Schulte when I suggested he only intended to use *legal filings* as the code with which he would hack the judicial system.

When dropping a laptop alters its BIOS

On June 1, Shroff wrote the court informing Judge Jesse Furman that a guard had accidentally dropped Schulte's discovery laptop, but asking for no further relief.

> We write to inform the Court that a guard at the MDC accidently dropped Mr. Schulte's laptop today, breaking it. Because the computer no longer functions, Mr. Schulte is unable to access or print anything from the

> laptop, including the legal papers due this week. The defense team was first notified of the incident by Mr. Schulte's parents early this afternoon. It was later confirmed in an email from BOP staff Attorney Irene Chan, who stated in pertinent part: "I just called the housing unit and can confirm that his laptop is broken. It was an unfortunate incident where it was accidentally dropped."
>
> Given the June 13, 2022 trial date, we have ordered him a new computer, and the BOP, government, and defense team are working to resolve this matter as quickly as possible. We do not seek any relief from the Court at this time.

I think Shroff is a formidable defense attorney and she has no patience for the carceral regime that her clients face, particularly someone under strict measures like Schulte. Which is why I find it so odd that she was so blasé about what might be viewed as intentional retaliation against Schulte, just days before trial, especially given Schulte's recent complaints about his access to the law library. A month earlier, after all, Shroff had described that efforts at détente with the jail had failed.

I'm especially puzzled about Shroff's response given the discrepancy between her explanation — sourced to Schulte's parents and the prison attorney, not anyone who could be held accountable for a false claim — and that of the government.

On June 6, DOJ explained its resolution of the laptop. Their explanation sounds nothing like a dropped laptop, at all. It sounds like an attempted hack.

> First, with respect to the defendant's discovery laptop, which he reported to be inoperable as of June 1, 2022 (D.E. 838), the laptop was operational and

> returned to Mr. Schulte by the end of the day on June 3, 2022. Mr. Schulte brought the laptop to the courthouse on the morning of June 3 and it was provided to the U.S. Attorney's Office information technology staff in the early afternoon. It appears that the laptop's charger was not working and, after being charged with one of the Office's power cords, the laptop could be turned on and booted. IT staff discovered, however, that the user login for the laptop BIOS1 had been changed. IT staff was able to log in to the laptop using an administrator BIOS account and a Windows login password provided by the defendant. IT staff also discovery [sic] an encrypted 15-gigabyte partition on the defendant's hard drive. The laptop was returned to Mr. Schulte, who confirmed that he was able to log in to the laptop and access his files, along with a replacement power cord. Mr. Schulte was admonished about electronic security requirements, that he is not permitted to enable or use any wireless capabilities on the laptop, and that attempting to do so may result in the laptop being confiscated and other consequences.

All the more so given one of the new details disclosed in the New Yorker profile: that in his moments of desperation to keep his contraband cell phone charged in jail back in 2018, Schulte figured out how to hot-wire the phone to the light switch.

> Schulte figured out a way to hot-wire a light switch in his cell so that it worked as a cell-phone charger. (The person who knew Schulte during this period praised his innovation, saying, "After that, all M.C.C. phones were charged that way.")

In recent months, Schulte has been making technical requests, such as for his own printer or a write-capable DVD which (he explicitly said) he wanted to use to transfer "other binary files" in addition to trial exhibits, that seemed an attempt to acquire equipment that could be used for other purposes. Here, in the guise of an accident caused by a guard, Schulte got his laptop, with its BIOS alteration, its encrypted compartment, and apparent attempts to use wireless capabilities, into the office of the people prosecuting him, then got it returned with a new power cord.

Among the things Schulte worked on at CIA was a tool to jump an air gap and compressing and exfiltrating data.

The expanding Pompeo subpoena

Then there's the way information has gotten to Schulte, who is under strict Special Administrative Measures that would normally limit news about his own case from getting shared with him (the following is not a commentary about the humanity or constitutionality of SAMs, which are arguably not either; it is an observation that they may not be working). In a filing purporting to represent Schulte's views as to why he needs to call Mike Pompeo as a witness, his stand-by attorneys laid out the following justification:

> Secretary Pompeo was Director of the CIA in May 2017 when WikiLeaks began disclosing Vault 7 and Vault 8. As noted in prior briefings to the Court, **[1]** Mr. Pompeo was immediately debriefed about the WikiLeaks disclosure and specifically informed that Mr. Schulte was an early suspect. He was also told that Mr. Schulte had a disciplinary history. Further, less than a week after the disclosure, Secretary Pompeo approved the substance of the first

> search warrant application, authorizing the FBI to make various statements therein, at least some of which later proved untrue.
>
> As such, Secretary Pompeo took an active role in the investigation against Mr. Schulte and has non-hearsay information that is relevant to the charges. Mr. Schulte also seek to inquire of Secretary Pompeo whether he directed his staff to consider charges against Mr. Schulte to the exclusion of anyone else or contrary to existing exculpatory evidence
>
> Further, while the government has sought to establish the grave harm caused by the leak, just months after it allegedly occurred, **[2]** Secretary Pompeo championed WikiLeaks' publication of the stolen DNS [sic] emails on social media. This disconnect, too, is ripe for examination.
>
> Finally, as recently as September 2021, **[3]** Secretary Pompeo continued to voice his views on the prosecution of leaks from WikiLeaks, see https://nationalpost.com/news/trump-pompeo-and-cia-agents-discussed-kidnappingassassinating-assange-in-revenge-for-vault-7-leak. Secretary Pompeo's evolving stance on the prosecution of leaks is relevant to the issues at trial. Accordingly, Mr. Schulte asks this Court to deny the government's application to preclude Secretary Pompeo's testimony. [my numbering]

In the past, I have argued that calling Pompeo as a witness is a reasonable request, for what I've marked as reason 2, above. As House Intelligence Chair, Mike Pompeo cheered WikiLeaks' release of emails by Russia from the DNC. He did so in July 2016, months after

Schulte is alleged to have transmitted the CIA files in early May 2016. That Pompeo's support of WikiLeaks, even when he had access to intelligence about them, did not prevent him from being confirmed as CIA Director undercuts claims about Schulte's perception of the particular damage leaking to WikiLeaks might do.

But the other two reasons are more suspect. Reason one, Pompeo's approval of early steps in the investigation, is only a measure of what he got briefed, and the briefer would be the more direct witness to the substance of that briefing (and given the seniority of some of the witnesses who testified at his first trial, likely already appeared as witnesses. But Pompeo's presumed briefing of the case *to Donald Trump* — before Trump almost blew the case by sharing those details with Tucker Carlson on the very day the FBI first searched Schulte — is another issue. I'm acutely interested in Trump's treatment of the attack on the CIA by a Russian-associated outlet in 2017, but it really doesn't indicate anything about Schulte's guilt or innocence.

The last reason — the claim published by Yahoo but never matched by another outlet that Pompeo responded to the initial Vault 7 release by asking about the possibility of assassinating Julian Assange — is a more dubious argument still. Remember: This is Schulte's standby counsel writing this filing. They're not under SAMs, Schulte is, but they're only his standby counsel, and so should only be posting things he can be privy to. The rationale for calling Pompeo is *presented as* Pompeo's comments, from September 2021, responding to the Yahoo story. Except the story linked — to a Canadian story on the Yahoo story published a day before Pompeo's response — doesn't reflect those 2021 comments from Pompeo at all. If Pompeo were really asked to testify about this, he would debunk parts of it, as his actual public comments about the story did. If the Yahoo story became an issue at trial, it might come out that the story repeats a claim (though nowhere near the most

inflammatory claim of the story) made publicly by a WikiLeaks surrogate in 2020, but never (AFAIK) made publicly elsewhere, and that Michael Isikoff had persistently suppressed details from the Stone prosecution that debunk large parts of the Yahoo story. That is, if the Yahoo story became an issue at Schulte's — or anyone else's — trial, it could easily be discredited, like several of the other stories used in WikiLeaks' campaign against Assange's extradition. But Schulte, who has purportedly read about this in spite of his SAMs, would like to make it an issue at his trial.

A minute note in the docket may indicate that the two sides settled this issue on Friday. So we're likely to be deprived of Pompeo's testimony for a second Schulte trial.

The [redacted] discovery

I find reasons one and three particularly interesting given a series of documents that presumably relate to a broader-than-publicly understood investigation into WikiLeaks. Schulte was provided materials from that investigation in discovery on April 6 or 8. Schulte sent Judge Furman a request on April 29 (perhaps not coincidentally, after a UK judge approved Assange's extradition, though the actual extradition decision remains pending before Priti Patel) asking to obtain *all* the discovery from that case, have it excluded from the protective order so he could use it at trial, and asking Furman to give Schulte an investigator so he could learn more about that investigation. In response to an order from Furman, the government responded on May 16. All the materials were docketed on May 25.

The materials are so heavily redacted as to offer little illumination to the subject. They do say, however, that the investigation "is neither known to the public nor to all of the targets of the investigation," suggesting that

at least one of those targeted is aware of it, and that DOJ is working with targets, not subjects. DOJ asserts that Schulte's claims about the utility of the evidence for his trial conflict. It also describes that Schulte wants to argue — falsely, DOJ asserts — that this evidence proves the Vault 7 materials were obtained by hackers. Given the original discovery letter and subsequent treatment, it is unclear to me whether this information is considered classified, or just confidential. But the government, unsurprisingly, argues that the material shouldn't be released.

> [B]ecause the [redacted] Investigation Materials relate to an ongoing criminal investigation, and their disclosure could cause serious harms to that investigation and other law enforcement interests.

The argument for Pompeo's testimony, above, came after DOJ responded to Schulte's request for more information. That is, Schulte's defense stretched beyond a completely legitimate claim that Pompeo's actions prove that even the CIA did not consider support for WikiLeaks disqualifying at the moment Schulte allegedly leaked the files, to claims that are little more than repetitions of Trumpist and WikiLeaks propaganda.

Meanwhile, Schulte is asking for a two day adjournment of trial after jury selection starting tomorrow, partly on account of the laptop, partly because the government has shifted the order in which they'll present witnesses, this time starting with Richard Evanchec, one of the FBI Agents who originally investigated the leak, rather than Schulte's colleagues at the CIA (among other things, doing so will foreground Schulte's easily debunked cover story, which he plans to tell himself in court).

Sometime this week, Schulte will have his moment in court, this time running his own defense and

exploiting whatever hacks — digital or legal — he has succeeded in launching over the last year or four. As Shroff says, Schulte's not bound by professional ethics in any way that would limit what arguments he makes. Schulte will undoubtedly attempt to feed the jury the kind of code that the legal system normally doesn't expect. We will then get to see whether such code causes the system to malfunction.