JOSHUA SCHULTE'S PLANS FROM JAIL: "#TOPSECRET#FUCKYOURTOPSECRET"

In response to an order from Judge Paul Crotty, the government laid out what evidence it wants to use from prison notebooks seized from accused Vault 7 leaker Joshua Schulte's jail cell. The whole filing is —as all descriptions of these notebooks have been — utterly damning.

For example, the filing explains a reference the government had earlier made: that Schulte had made reference to non-public information about what WikiLeaks had received in the Vault 7 leak. Schulte wrote a note sometime in July 2018 suggesting that if "you" needed help, they should ask WikiLeaks for Schulte's "code."

> "Ask WikiLeaks" (014099) (undated): In the middle of the page, the defendant writes, "If you need help ask WikiLeaks for my code."3 The defendant's direction to consult WikiLeaks about his "code" is admissible as Nonpublic Information Evidence, because it is a statement that WikiLeaks is in possession of source code for tools upon which the defendant worked and that are contained in the back-up file that was stolen, even though WikiLeaks has not publicly disclosed that it possesses any source code for all of the tools. Schulte's knowledge of non-public aspects of the information that was given to WikiLeaks helps to demonstrate that he was the one who gave that information to WikiLeaks in the first place.

Schulte wrote this in the second person, suggesting he was advising (or planning to advise) someone to use source code he wrote. He

is known to have worked on obfuscation tools and a remote USB exfiltration tool. If he did intend that as instruction, he assumed the person in question would have been able to consult directly with WikiLeaks. It's unclear to what end Schulte was imagining advising someone to use obfuscation or hacking tools written for the CIA.

In any case, the government claims that's proof that Schulte knows exactly what was in WikiLeaks' possession.

A later entry suggests Schulte and someone else — "we" — were trying to compromise email, possibly his own CIA email.

> "What We Expect to Find in Emails" (014136) (undated): At the top of this page, the defendant writes "What we expect to find in emails." On the remainder of the page, the defendant writes a list of items, many of which contained classified information. This portion of the Blue Notebook is admissible as Intent Evidence and MCC Classified Information Evidence, because it shows the defendant cataloguing classified information that, if publicly disclosed, would likely be harmful to the United States. Indeed, some of the categories of information identified by the defendant on this page—such as certain operations—is the same as the classified information contained in the Fake Authentication Tweet, which serves to show that the defendant's intent was to collect these materials for dissemination, not for any legitimate purpose related to his defense.

Later, the letter describes a part of Schulte's planned Information War on the United States, probably dating to late August or early September 2018, one he wanted to roll out in a tweet with the hash tag, "#TopSecret#FuckYourTopSecret."

> Over these three pages, Schulte wrote the following. At the top of the first page, Schulte wrote "#TopSecret#FuckYourTopSecret," and under that draws an arrow to the phrase "or dump the secrets here:". At the top of the page Schulte also wrote "establish credibility," and, underneath that appears another version of the Fake Authentication Tweet. Later, the defendant recommends to U.S. intelligence agency employees to "send all your govt's secrets here: WikiLeaks" until the U.S. government "honors" their service. As with the last entry, this is entry contains MCC Classified Information Evidence in the form of the Fake Authentication Tweet. In addition, the instruction to intelligence agency employees to give their "secrets" to WikiLeaks is Intent Evidence.

Effectively, the government seems to be arguing, Schulte planned to use a Twitter account in the name of Jason Bourne to encourage US intelligence agency employees to leak information to WikiLeaks, something Julian Assange did himself in a post-Snowden 2013 speech. Not only does this suggest Schulte was shifting into recruitment mode, but it validates the motive the government claims he himself had for leaking the CIA's hacking tools, because the CIA didn't "honor" his service. That's one of the classic recruitment motives (of money, ideology, compromise, and ego, the latter).

These parts of Schulte's prison notebooks, then, suggest he was doing more than just posting his blogposts and sharing a CIA network diagram from jail. He was at least *imagining* he might use tools he wrote for the CIA to steal emails full of classified secrets and also recruit others to feed WikiLeaks with more classified information over Twitter.

Schulte's team, in one of the only filings they've submitted that makes a decent point in

Schulte's defense, finally offered an explanation for why this may not be as damning as it looks.

In yet another bid to get Paul Rosenzweig's testimony showing how Schulte's actions fit into a pattern that make look WikiLeaks look like a criminal organization, they argue that Rosenzweig's testimony that leaking to WikiLeaks would exhibit an intent to damage the US could only work if the government first proved that Schulte knew how WikiLeaks worked.

> The Court ruled, in relevant part, that "[a]n understanding of the WikiLeaks organization and how it operates is directly relevant to the allegation that, In transmitting Classified Information to WikiLeaks, Schulte intended or had reason to believe there would be injury to the United States." Dkt. 256, at 4. This ruling makes sense only if the government first presents foundational evidence showing that Mr. Schulte knew how WikiLeaks was organized and operated. Absent such evidence showing what Mr. Schulte knew, expert testimony about these subjects would be totally disconnected from—and therefore would have no bearing on—Mr. Schulte's state of mind.
>
> [snip]
>
> Here, absent proof that Mr. Schulte was aware of how WikiLeaks was organized or functioned, Mr. Rosenzweig's testimony about those subjects, even if accurate and admissible under Fed. R. Evid. 702, would be irrelevant to what Mr. Schulte "intended or had reason to believe" when he allegedly leaked information to WikiLeaks in 2016. As in Kaplan, it would be error to admit this testimony without the required connection to what Mr. Schulte actually knew.
>
> The same principle applies to Mr.

> Rosenzweig's purported testimony about harm ostensibly caused by prior WikiLeaks revelations. If Mr. Schulte did not know in 2016 about the prior revelations or the harm they supposedly caused to the United States, any expert testimony about those revelations and resulting harm is irrelevant (and unfairly prejudicial under Rule 403).

In earlier filings, the government has made much of the fact that August 4, 2016 is the first or one of the first times Schulte ever searched Google for information on WikiLeaks. And, trust me, this guy recorded everything in his Google searches. So, the defense could argue, Schulte didn't even begin to learn about the outlet he had leaked to until three months after he leaked the files to them (nevermind how he figured out how to get it to them).

This only works to limit the applicability of Rosenzweig's testimony for the CIA leaks, not the leaks and attempted leaks from MCC. Plus, Schulte's claim to have been part of Anonymous — whether or not it's true — would amount to a claim that he operated in an environment where he would have learned of WikiLeaks in chatrooms. But it's not clear the government could prove that.

Whether or not they can show Schulte's actions are part of a longer campaign by WikiLeaks to encourage intelligence professionals to leak to WikiLeaks to avenge slights by the government, the notebooks are even more damning than the government has previously revealed.

As I disclosed in 2018, I provided information to the FBI on issues related to the Mueller investigation.