~~SECRET//NOFORN~~

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	
- v. -	S2 17 Cr. 548 (PAC)
JOSHUA ADAM SCHULTE,	
Defendant.	

THE GOVERNMENT'S OMNIBUS OPPOSITION TO THE DEFENDANT'S SUPPRESSION MOTIONS

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
Attorney for the United States of America

Matthew Laroche
Sidhardha Kamaraju
Assistant United States Attorneys
Scott McCulloch
Trial Attorney, National Security Division
Of Counsel

~~SECRET//NOFORN~~

TABLE OF CONTENTS

~~SECRET//NOFORN~~

PRELIMINARY STATEMENT

The Government respectfully submits this omnibus brief in opposition to defendant Joshua Adam Schulte's motions to suppress evidence seized from (i) his residence in New York City and certain electronic accounts (Dkt. 109) (the "Residence Motion"), and (ii) the Metropolitan Correctional Center (Dkt. 98) (the "MCC Motion" and together with the Residence Motion, the "Defense Motions"). For the reasons set forth below, Schulte's motions are entirely without merit and should be denied without a hearing.[1]

On March 7, 2017, the organization WikiLeaks.org ("WikiLeaks") began one of the most significant disclosures of U.S. government classified information in the history of the nation and claimed that more was coming. That disclosure, which was followed by 25 more, included information about sensitive cyber-tools from the Central Intelligence Agency (the "CIA") that significantly damaged the national security of the United States by not only disclosing certain CIA intelligence-gathering methods, but also by giving hostile actors a mechanism to turn these potent cyber weapons against the United States. The Federal Bureau of Investigation ("FBI") immediately began an investigation, seeking not only to catch the perpetrator, but also to stem further disclosures and to assess precisely how large a leak had occurred.

---

[1] Because portions of this brief contain classified information, the Government is filing a redacted version of this brief publicly. The Government is separately providing an unredacted copy of this brief to the Court and defense counsel under seal.

"Res. Br." refers to the defendant's brief in support of the Residence Motion; "MCC Br." refers to the defendant's brief in support of the MCC Motion; "Bellovin Decl." refers to the declaration of Dr. Steven M. Bellovin in support of the Residence Motion; "Shroff Decl." refers to the unclassified declaration of defense counsel in support of the Defense Motions; "Shroff Classified Decl." refers to the classified declaration of defense counsel in support of the Defense Motions; and "Ex." refers to an exhibit to this opposition brief. Exhibits K through N to this brief contain classified information and, as a result, are being filed under seal. Exhibit O is an image of apparent child pornography that the Government is providing to the Court for inspection under seal. Exhibit O is (and has previously been) available to defense counsel to review at their request.

Within days of the initial disclosure, the FBI secured a search warrant for Schulte's home, among other warrants. As that warrant detailed, Schulte was a disgruntled former CIA employee with an expertise in developing tools to covertly copy electronic data, was one of a small number of CIA employees who had authorized access to the leaked information, had illegally manipulated the CIA's computer systems on at least two occasions in the past to gain unauthorized access to sensitive CIA material, had flouted CIA security protocols, and was scheduled to take only his second trip ever out of the country shortly after the March 7 Leak by WikiLeaks. Then, during the search of Schulte's home desktop computer, the FBI uncovered an image that depicted a child engaged in sexual acts and sought a second search warrant, this time to seize evidence of child pornography. But even after ultimately uncovering sufficient evidence to charge Schulte with, among other crimes, offenses under the Espionage Act based on the WikiLeaks disclosures and child pornography offenses, the FBI's investigation of Schulte did not end. Instead, from a federal detention facility, Schulte continued his "information war" against the United States, smuggling in contraband cellphones and using encrypted email accounts to disclose and attempt to disclose more classified information. The FBI thus executed more search warrants to determine precisely how Schulte had continued his campaign against the United States from prison.

Despite the urgency of this national security investigation, the FBI exercised remarkable caution and candor in securing search warrants in this case: In the affidavit for the very first search warrant for Schulte's home, the FBI affiant laid out a compelling case for Schulte's complicity in the leak, but also made clear the limits of the FBI's knowledge at that time. When the FBI discovered a single image of possible child pornography on Schulte's desktop computer, the FBI stopped its review and sought another search warrant, even though the FBI already had a search warrant that would have authorized them to continue to search the computer. Even during an

urgent search of Schulte's cell at a time when the FBI suspected (correctly) that Schulte was continuing to disclose classified materials from prison, the FBI refrained from searching documents that purported to be privileged (most of which were not), so that a wall review team could be put in place to protect the defendant's attorney-client privilege.

Despite this, Schulte now seeks to suppress evidence seized pursuant to those warrants based on a standard that has no basis in the law or the facts. Schulte claims that the first affidavit to search his home was deliberately misleading and failed to establish probable cause, but he ignores the actual language of the affidavit, the substantial evidence of his guilt that the affidavit described, and the fact that the overwhelming majority of information that he claims renders the affidavit incorrect originated *after* the affidavit was executed. With respect to the child pornography warrants, the FBI's discovery of an illicit image on Schulte's home computer was ample probable cause to search for and seize any additional images of child pornography (of which the FBI discovered thousands). Moreover, even if the child pornography warrants were deficient, the child pornography was discovered in places on Schulte's home computer that the FBI inevitably would have searched pursuant to the original espionage warrant. With respect to evidence seized from Schulte's prison cell, the FBI followed the appropriate procedures to search for evidence of Schulte's "information war" while ensuring that the FBI did not intrude on Schulte's attorney-client privilege. Finally, with respect to all of these warrants, because the FBI acted in good faith, none of the seized evidence should be suppressed.

In the end, Schulte's motion does not seek to ensure that the FBI acted honestly, which it did. Rather, he would have the agents act as soothsayers and defense counsel, foreseeing events that had not yet developed and indulging implausible defense theories. The law, however, does not require that. Schulte's motions should be denied without a hearing.

BACKGROUND

The charges in this case stem from a long-term investigation into WikiLeaks's disclosure of classified CIA information. In particular, between March 7 and November 17, 2017, WikiLeaks made 26 separate disclosures that included classified CIA information (the "Leaks"). The Leaks contained, among other things, highly sensitive CIA information (the "Classified Information") including detailed descriptions of certain CIA tools. The Leaks' impact on the CIA's intelligence gathering activities and the national security of the United States was catastrophic.

The FBI's investigation began immediately after WikiLeaks's initial March 7, 2017 disclosure (the "March 7 Leak"). As part of that investigation, the FBI quickly developed facts establishing probable cause that Schulte was responsible for the theft of the Classified Information. As a result, the FBI executed a series of search warrants on Schulte's New York City residence (the "Residence") and electronic accounts. These included a search warrant, executed on March 13, 2017, authorizing the covert search of the Residence and the electronic media therein (the "Covert Warrant," attached as Exhibit A); as well as warrants executed in the early morning of March 14, 2017, authorizing the overt search of Schulte's Residence (the "Overt Warrant," attached as Exhibit B) and the search of Schulte's Google, Reddit, and Github electronic accounts (the "Electronic Accounts Warrant," and together with the Covert Warrant and the Overt Warrant, the "Espionage Warrants"). Moreover, as part of the FBI's review of Schulte's desktop computer and servers recovered from his Residence, the FBI developed facts establishing that Schulte was engaged in child pornography and copyright infringement offenses. As a result, on April 14 and May 10, 2017, the FBI executed warrants authorizing the search of electronic media seized from the Residence for evidence of those offenses (the "Supplemental Warrants," attached as Exhibit C and D, respectively). On May 10, 2017, the FBI executed another warrant to search Schulte's

Google account (the "CP Electronic Account Warrant," attached as Exhibit E, and together with the Espionage Warrants and Supplemental Warrants, the "2017 Warrants"), for evidence of espionage, child pornography, and copyright infringement offenses.

Based on the information gathered as part of the investigation, Schulte was charged with espionage and other offenses related to the Leaks, as well as child pornography and copyright offenses. *See* S1 17 Cr. 548. While those charges were pending and Schulte was detained at the MCC, the Government learned that Schulte and other inmates had cellphones (the "Contraband Cellphones") smuggled into the prison and that Schulte may have been using the Contraband Cellphones to further disclose classified information. As a result, the Government quickly obtained a series of search warrants to investigate that conduct (the "MCC Warrants, and together with the 2017 Warrants, the "Challenged Warrants"). These included a warrant authorizing the search of the MCC for the Contraband Cellphones and other classified documents (the "MCC Premises Warrant," attached as Exhibit F), as well as a subsequent warrant authorizing a wall team to review certain of the documents seized during the search of the MCC (the "MCC Wall Warrant," attached as Exhibit G). Based on the evidence gathered from the MCC, the FBI executed a series of other warrants for electronic accounts and devices Schulte used to transmit classified information from prison (the "Encrypted Email Warrant," attached as Exhibit H, the "Social Media Warrant," attached as Exhibit I, and the "Laptop Warrant," attached as Exhibit J).

Based on Schulte's conduct, on October 31, 2018, the Government filed a superseding indictment charging him with, in addition to the charges contained in the S1 Indictment, one additional count of unlawfully disclosing and attempting to disclose classified information and one count of contempt of court for willfully violating a court order. *See* S2 17 Cr. 548 (PAC).

~~SECRET//NOFORN~~

I. EVIDENCE SEIZED PURSUANT TO THE ESPIONAGE WARRANTS SHOULD NOT BE SUPPRESSED

Schulte's motion to suppress the evidence seized pursuant to the Espionage Warrants is based entirely on his challenges to the affidavit supporting the Covert Warrant (the "Covert Affidavit"). Schulte's motion is meritless—most of what he claims to be false in the Covert Affidavit is true, any purported errors in the Affidavit are nevertheless immaterial and were not the result of an intent to deceive the magistrate judge, and, in any event, the FBI relied on the Espionage Warrants in good faith. Schulte's motion to suppress the evidence seized pursuant to the Espionage Warrants should be denied as a matter of law and without a hearing.[2]

A. Relevant Background

1. The Covert Warrant

In support of its application for the Covert Warrant, which was executed less than one week after the initial March 7 Leak, the Government submitted an affidavit by Special Agent Jeff D. Donaldson (the "Covert Affidavit"). (Ex. A). As detailed in the Covert Affidavit, Agent Donaldson is an experienced counterespionage investigator. (*Id.* ¶ 1). The Covert Affidavit described Agent Donaldson's work in the field of counterespionage since 2010 and his prior experience investigating offenses involving espionage. (*Id.*). The Affidavit also described Agent Donaldson's familiarity with the methods used by individuals engaged in espionage offenses, including the use of computers. (*Id.*).

---

[2] In addition, while the Government does not believe a *Franks* hearing is appropriate, should the Court hold such a hearing, the Government would establish that the evidence seized pursuant to the Espionage Warrants would inevitably have been discovered because, as the investigation proceeded, the FBI gathered substantially more evidence against Schulte from CIA computer systems and documentary evidence, and it would have included that information in any subsequent warrant applications. As a result, the inevitable discovery doctrine also applies, and this evidence should not be suppressed on that ground as well. *See infra* pp. 51-52.

The Covert Affidavit provided substantial information establishing probable cause that Schulte stole the Classified Information. In particular, the Covert Affidavit provided an overview of the March 7 Leak, as well as assessments about how and when the Classified Information was potentially stolen. The Covert Affidavit then described the numerous facts demonstrating that Schulte was responsible for stealing it and explained why a covert search was warranted.

a. Overview of the March 7 Leak and the Potential Methods of Exfiltration

Agent Donaldson explained that on March 7, 2017, WikiLeaks had disclosed more than 8,000 documents and files that contained classified information belonging to the CIA. WikiLeaks claimed in its accompanying press release that, among other things, the March 7 Leak constituted the "first full part" of a series of additional releases and that the "collection" obtained by WikiLeaks amounted to "more than several hundred million lines of code" and revealed the "entire hacking capacity" of the CIA. (*Id.* ¶¶ 7(b)-(c), 8(a)).

Agent Donaldson also explained that the March 7 Leak was stored on a computer network (the "LAN") used exclusively by a particular group within the CIA (the "CIA Group"). (*Id.* ¶ 9). The LAN was an isolated local area computer network and was physically separated from unsecured networks, such as the public Internet. (*Id.* ¶ 9(a)). As of March 2016, fewer than 200 employees—those then assigned to the CIA Group—had access to the LAN. (*Id.* ¶ 9).

Agent Donaldson assessed that the March 7 Leak was likely stolen from the LAN's server that was used to store backup data (the "Back-Up Server"). (*Id.* ¶ 10). He explained that the CIA Group's work was backed up through an automated process, on an approximately daily basis, to the Back-Up Server, and that each daily backup was akin to an electronic "snapshot" of the data on that particular date. (*Id.* ¶ 10(a)). Because the March 7 Leak contained numerous iterations (or

snapshots) of the same or similar data distinguished by date, Agent Donaldson stated that the information was likely taken from the Back-Up Server. (*Id.* ¶ 10(d)).

With respect to the timing of the theft, Agent Donaldson stated that the March 7 Leak "appears to have been stolen from the CIA [Group] sometime between the night of March 7, 2016 and the night of March 8, 2016." (*Id.* ¶ 8(c)). This assessment was "based on preliminary analysis of the timestamps associated with the Classified Information which indicates that March 7, 2016 was the latest (or most recent) creation or modification date associated with the Classified Information." (*Id.* ¶ 8(c)); *see also id.* ¶ 8(c)(iii) n.1 (stating that this assessment was based on a "preliminary analysis"). Notably, Agent Donaldson made clear that "[i]t is of course possible that the Classified information was copied later than March 8, 2016 even though the creation/modification dates associated with it appear to end on March 7, 2016." (*Id.* ¶ 8(c)(iii) n.1). "For example, the individual who copied and removed the data could have limited his or her copying to data that was modified or created on or before March 7, 2016." (*Id.*).

b. Probable Cause That Schulte Stole the March 7 Leak and That Evidence Would Be Found in His Residence

After outlining the likely timing and method of exfiltration of the March 7 Leak, Agent Donaldson set forth facts showing that Schulte had stolen the Classified Information.

First, Agent Donaldson explained that the LAN "was designed such that only those employees who were specifically given a particular type of systems-administrator access ('Systems Administrators') could access the Back-Up Server" and that, as of approximately March 2016, Schulte was one of three Systems Administrators. (*Id.* ¶ 11-12(a)). Agent Donaldson caveated this information, stating that it was "possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server" by, for example, stealing and using the username and password of a designated Systems Administrator or gaining

access to the Back-Up Server by finding a "back-door." (*Id.* ¶ 11(b) n.4). Agent Donaldson also stated that "based on a preliminary review," the March 7 Classified Information appeared to contain the names and/or pseudonyms of the other two Systems Administrators, as well as other CIA employees, but not Schulte's name and/or pseudonym. (*Id.* ¶ 12(b)).[3]

Second, Agent Donaldson explained that Schulte was present at the CIA on March 7 and 8, 2016—when the FBI assessed the Classified Information in the March 7 Leak was taken. (*Id.* ¶ 13(a)). On March 8, several of Schulte's colleagues at the CIA Group were away from the office including, two of the three employees who had direct line-of-sight to Schulte's desk and computer. (*Id.* ¶ 13(a)-(b)). Moreover, on March 8, one of the two other Systems Administrators did not have LAN access, while Schulte and the third administrator did have LAN access. (*Id.* ¶ 13(d) n.5).

Third, Agent Donaldson stated that Schulte had engaged in several unauthorized actions on the LAN in April and May 2016, which resulted in CIA management reprimanding Schulte on two occasions. In particular, on or about April 4, 2016, around the time Schulte was reassigned to another branch within the CIA Group, "many of Schulte's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a Systems Administrator." (*Id.* ¶ 14). Also on or about April 4, 2016, Schulte's computer access to a specific developmental project ("Project-1") was also revoked. Although Schulte retained read-only access to Project-1, principal responsibility for Project-1 was transferred to another CIA Group employee. (*Id.* ¶ 14(a)-(b)).[4] However, less than two weeks later, on or about April 11, 2016, Schulte "unilaterally and without authorization logged onto the CIA Group's LAN and reinstated his own administrative privileges."

---

[3] Certain CIA employees use pseudonyms to protect their identity.

[4] Agent Donaldson noted that Schulte retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility. (*Id.* ¶ 14(b) n.6).

(*Id.* ¶ 15).[5] As a result of this conduct, on or about April 18, 2016, Schulte received a notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. Schulte also signed an acknowledgment that "'individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system.'" (*Id.* ¶ 15(b)). That notice also instructed Schulte, "do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed." (*Id.*).

Despite the unambiguous warnings in the notice that Schulte acknowledged, a little more than a month later, on or about May 26, 2016, Schulte received access to Project-1 through another employee and then used that access to "unilaterally and without authorization revoke the computer access permissions of all other CIA Group employees to work on Project-1." (*Id.* ¶ 14(c)). Once this conduct was discovered, Schulte was issued a letter of warning that stated: "You were aware of the policy for access and your management's lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges." (*Id.* ¶ 14(c)(ii)). Agent Donaldson stated that Schulte disagreed with some of the warning's conclusions and refused to sign the form. (*Id.* ¶ 14(c)(iii)).

Fourth, Agent Donaldson stated that Schulte was angry based on how the CIA responded to Schulte's March 2016 complaint that another employee had threatened him. (*Id.* ¶¶ 17, 18). In particular, Schulte "expressed deep unhappiness about the way the CIA responded to the alleged threat"; "threatened legal action against the CIA for its handling of the situation"; "repeatedly stated that he felt that he was being punished by the CIA management for reporting the alleged

[5] As the Government noted in the Disclosure Letter, while Schulte lost certain privileges to Project-1 on or about April 4, 2016 and was no longer acting as a Systems Administrator, Schulte retained his System Administrator Privileges for some time after that.

threat"; "informed CIA security that, if 'forced into a corner' he would proceed with a lawsuit against the CIA"; and "repeatedly threatened that he or his lawyer would go to the media." (*Id.* ¶ 17). Moreover, Schulte "had removed an internal CIA document from CIA facilities" about his complaint "despite being told multiple times by CIA security officials not to do so." (*Id.*).

Agent Donaldson described how many of Schulte's former colleagues confirmed his "deep unhappiness" and inappropriate handling of CIA information, stating "[s]ome (but not all) colleagues independently reported that Schulte's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016" (*id.* ¶ 18(a)); "[m]ultiple colleagues stated that Schulte had indicated that he felt aggrieved by the CIA in a number of respects" (*id.* ¶ 18(b)); "[s]ome also reported that they believed Schulte to be untrustworthy and potentially subject to outside coercion" (*id.*); and "[s]ome (but not all) colleagues also reported that Schulte's security practices were lax, and that Schulte tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems" (*id.* ¶ 18(c)). Notably, Agent Donaldson stated that some colleagues disagreed and "affirmatively reported that they believed that Schulte was, in fact, trustworthy." (*Id.* ¶ 18(b)).

Fifth, Agent Donaldson discussed the circumstances of Schulte's resignation from the CIA in November 2016, including a letter and email he wrote complaining about his treatment. (*Id.* ¶¶ 19-20). On October 12, 2016, Schulte sent an email to another CIA Group employee with the subject line "ROUGH DRAFT of Resignation Letter *EYES ONLY*," which attached a three-page, single-spaced letter (the "Letter"). (*Id.* ¶ 19(a)). In the Letter, Schulte stated that the CIA Group management had unfairly "veiled" CIA leadership from various of Schulte's "concerns about the network security of the CIA Group's LAN" and that "[t]hat ends now. From this moment

forward you can no longer claim ignorance; you can no longer pretend that you were not involved." (*Id.* ¶ 19(a)(ii)). The Letter also stated that Schulte was resigning because management had "'ignored'" issues he had raised about "'security concerns,'" including that the LAN was "'incredibly vulnerable' to the theft of sensitive data." (*Id.* ¶ 19(a)(iii)). In particular, Schulte stated that the "inadequate CIA security measures had 'left [the CIA Group's LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.'" (*Id.* ¶ 19(a)(iv)).

Agent Donaldson noted that Schulte did not appear to send the Letter. (*Id.* ¶ 19(b)). However, on November 10, 2016, Schulte's last day at the CIA, Schulte sent an internal email to the CIA's Office of Inspector General ("OIG"), which Schulte marked "Unclassified," advising that he had been in contact with the U.S. House of Representatives' Permanent Select Committee on Intelligence regarding his complaints about the CIA (the "OIG Email"). (*Id.* ¶ 19(c)). The OIG Email raised many of the same complaints in the Letter, including "the CIA's treatment of him and its failure to address the 'security concerns' he had repeatedly raised in the past." (*Id.* ¶ 19(c)(i)). Although Schulte had labeled the OIG Email "Unclassified," the CIA determined that the OIG Email did in fact contain classified information. (*Id.* ¶ 19(c)(iii)). Schulte nevertheless printed and removed the email from the CIA when he left that day. (*Id.* ¶ 19(c)(ii)).

Sixth, Agent Donaldson summarized communications between Schulte and some of his former colleagues that occurred immediately after the March 7 Leak. (*Id.* ¶ 20). In particular, Schulte repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group employees and, among other things, (i) repeatedly asked about the status of the investigation (*id.* ¶ 20(a)); (ii) requested more details on the information that was disclosed (*id.* ¶ 20(b)); (iii) asked his colleagues' personal opinions regarding who within the CIA Group stole the

information (*id.* ¶ 20(c)); (iv) asked what CIA Group employees were saying about the disclosure (*id.*); (v) repeatedly denied involvement in the disclosure (*id.* ¶ 20(d)); and (vi) said he believes he is a suspect in the theft of the Classified Information in the March 7 Leak (*id.* ¶ 20(e)).

Seventh, Agent Donaldson stated that Schulte was scheduled to leave the country for only the second time on March 16, 2017, with return travel booked for a few days later. (*Id.* ¶ 21).

Eighth, in the Covert Affidavit, Agent Donaldson made several observations based on his previously described (and extensive) training and experience. These observations included that individuals who engage in the unauthorized theft, retention, and transmission of classified information "often use computers and other electronic devices to store documents and records relating to their illegal activity." (*Id.* ¶ 24). In particular, individuals engaged in these activities "use electronic devices to, among other things, store copies of classified documents or materials; engage in email correspondence relating to their illegal activity; store contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; and/or store records of illegal transactions involving classified documents." (*Id.*). Agent Donaldson also assessed that individuals engaged in these activities "in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data" (*id.* ¶ 25), and that computer files and their remnants "can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet (*id.* ¶ 27). Agent Donaldson also stated that Schulte's credit card records and surveillance confirmed that he lived at the Residence. (*Id.* ¶ 23).

c. Necessity for the Covert Search of the Residence

The Covert Affidavit also sought authorization to search the Residence without advanced notice to Schulte. In support of this request, Agent Donaldson restated his belief, based on the

foregoing sections, that Schulte had "stolen a substantial amount of classified information and transmitted that information to those not authorized to receive it, thereby endangering the nation's national security." (*Id.* ¶ 37(a)). Moreover, Agent Donaldson stated that Schulte "likely engaged in these activities by using sophisticated computer skills to exfiltrate a substantial amount of data onto a removable drive and then covertly removed that drive from the CIA." (*Id.* ¶ 37(b)). As a result, providing Schulte advance notice of the search "may allow him to destroy evidence of his crimes on electronic devices by, for example, deleting drives or activating encryption programs that would make his devices virtually impossible to access." (*Id.* ¶ 37(c)).

In support of this request, Agent Donaldson discussed the nature of the investigation at the time. In particular, he stated that the investigation "is on-going, and remains extremely sensitive" and that "[t]he FBI is continuing to review an enormous volume of electronic evidence, much of which remains highly classified and extremely sensitive." (*Id.* ¶ 39). Moreover, based on WikiLeaks's press release, Agent Donaldson assessed that additional CIA information may have been stolen and provided to WikiLeaks or others. This assessment was based on the fact that WikiLeaks had "claimed to have refrained from publishing additional information they purport to possess such as armed cyberweapons" and also claimed to have anonymized some identifying information potentially relating to the names of covert CIA operatives and possibly covert United States Government locations. (*Id.*). Based on this information, and the fact that Schulte was expected to travel overseas imminently, Agent Donaldson sought covert authorization "to minimize the possibility" that Schulte would flee or destroy evidence. (*Id.*).

2. The Overt Warrant and Subsequent Disclosures

On March 13, 2017, after the Covert Warrant was signed, FBI agents covertly entered the Residence and observed, among other things, computers, servers, and other electronic devices (the

"Electronic Devices"). Because forensically imaging the Electronic Devices would have taken significant time and risked alerting Schulte to the investigation, law enforcement officers terminated the search. Although the Covert Warrant authorized the FBI to search the Residence overtly if necessary (Ex. A ¶ 37 (requesting authorization to search the Residence covertly "or if [law enforcement] deem[s] covert execution impracticable to execute the search warrant overtly without further order of the Court")), Agent Donaldson nevertheless sought the Overt Warrant out of an abundance of caution. The Overt Warrant was signed during the early morning hours of March 14, 2017, and the FBI executed the warrant the same day.

On September 18, 2018, the Government sent a letter to Schulte (the "Disclosure Letter") in which the Government noted that it had developed information through its ongoing investigation after Agent Donaldson swore to the Covert Affidavit that was relevant to some of the statements in the Covert Affidavit. (Shroff Decl., Ex. F).

B. Applicable Law

1. The Standard for Reviewing Probable Cause

Consistent with the Fourth Amendment, a search warrant must "describe with particularity the place to be searched and the persons or things to be seized." *United States v. Rosa*, 626 F.3d 56, 61 (2d Cir. 2010). In considering a request for a search warrant, "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Such determinations must be approached in a practical way, *id.* at 231-32, because "probable cause is a flexible, common-sense standard," *Texas v. Brown*, 460 U.S. 730, 742 (1983). Moreover, the training and experience of law enforcement agents bear significantly on probable cause

determinations. *See Gates*, 462 U.S. at 232. Inferences drawn by law enforcement agents based on facts known to them, the totality of the circumstances, and their training and experience may all support a probable cause finding. *Id.* at 231-32; *see also United States v. Gaskin*, 364 F.3d 438, 457 (2d Cir. 2004) ("[C]ourts recognize that experience and training may allow a law enforcement officer to discern probable cause from facts and circumstances where a layman might not.").

Once a search warrant has issued, the issuing judge's "determination of probable cause should be paid great deference by reviewing courts." *Gates*, 462 U.S. at 236 (internal quotation marks omitted). "[A]fter-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review." *Id.* Thus, "'[a]lthough in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants.'" *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993) (quoting *United States v. Ventresca*, 380 U.S. 102, 109 (1965)). "[S]o long as the magistrate had a 'substantial basis for . . . conclud[ing]' that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more." *Gates*, 462 U.S. at 236 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)); *see also United States v. Singh*, 390 F.3d 168, 181 (2d Cir. 2004) ("In reviewing a magistrate's probable cause determination, we accord substantial deference to the magistrate's finding and limit our review 'to whether the issuing judicial officer had a substantial basis for the finding of probable cause.'" (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993)).

2. The *Franks* Doctrine

A search warrant affidavit is presumed reliable. *Franks v. Delaware*, 438 U.S. 154, 171 (1978). Under *Franks*, "[t]o suppress evidence obtained pursuant to an affidavit containing erroneous information, the defendant must show that: '(1) the claimed inaccuracies or omissions

are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the [issuing] judge's probable cause finding.'" *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000) (citing *Franks*, 438 U.S. at 164-172). The defendant must establish both components—*i.e.*, materiality and intent—by a preponderance of the evidence. *See United States v. Klump*, 536 F.3d 113, 119 (2d Cir. 2008). "The *Franks* standard is a high one." *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991).

The intent component of the *Franks* inquiry is a "subjective test" that "looks to the mental states of mind of government officials." *United States v. Rajaratnam*, 719 F.3d 139, 153 (2d Cir. 2013) (reversing suppression order "because the District Court failed to consider the actual states of mind of the wiretap applicants"). The defendant must present "credible and probative evidence" that any misrepresentations and omissions were "'designed to mislead'" or were "'made in reckless disregard of whether [they] would mislead.'" *Id.* at 154 (quoting *United States v. Awadallah*, 349 F.3d 42, 68 (2d Cir. 2003)). "To prove reckless disregard for the truth, the defendant[] [must] prove that the affiant in fact entertained serious doubts as to the truth of his allegations." *Id.* (quoting *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir. 2001)). Findings of "misstatements or omissions caused by 'negligence or innocent mistake[s]' do not warrant suppression." *Id.* at 153 (quoting *Franks*, 438 U.S. at 171).

Because "[a]ll storytelling involves an element of selectivity," *Wilson v. Russo*, 212 F.3d 781, 787 (3d Cir. 2000), "'[a]n affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation,'" *Awadallah*, 349 F.3d at 67-68 (quoting *United States v. Colkley*, 899 F.2d 297, 300-01 (4th Cir. 1990)). Thus, "*Franks* claims based on omissions are less likely to justify suppression than claims of intentionally or recklessly false assertions." *United States v. Vilar*, 2007 WL 1075041, at *27 (S.D.N.Y. 2007).

The materiality of an error in a search warrant affidavit is "gauge[d] . . . by a process of subtraction: To determine if the false information was necessary to the issuing judge's probable cause determination, *i.e.*, material, 'a court should disregard the allegedly false statements and determine whether the remaining portions of the affidavit would support probable cause to issue the warrant.' If the corrected affidavit supports probable cause, the inaccuracies were not material to the probable cause determination and suppression is inappropriate." *Awadallah*, 349 F.3d at 64 (citing *Canfield*, 212 F.3d at 718). "The ultimate inquiry is whether, after putting aside erroneous information and material omissions, there remains a residue of independent and lawful information sufficient to support probable cause." *Id.* (internal quotation marks omitted).

Even to merit a hearing on the issue, a defendant must make "'a substantial preliminary showing' that a 'deliberate falsehood' or a statement made with 'reckless disregard for the truth' was included in the warrant affidavit, and the statement was 'necessary to the judge's probable cause finding.'" *United States v. Falso*, 544 F.3d 110, 134 (2d Cir. 2008) (quoting *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998)); *see United States v. Carter*, 2009 WL 765004, at *2 (2d Cir. 2009) ("Carter was not entitled to a hearing because he made no substantial preliminary showing that a deliberate falsehood or statement made with reckless disregard for the truth was included in the warrant affidavit and the statement was necessary to the judge's finding of probable cause." (internal quotation marks omitted)). "The burden to obtain such a hearing is a heavy one, and such hearings are exceedingly rare." *United States v. Melendez*, 2016 WL 4098556, at *7 (S.D.N.Y. 2016); *see also Franks*, 438 U.S. at 171-72 ("To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth . . . accompanied by an offer of proof."); *United States v. Keith*, 2016 WL 1644370,

at *2 (S.D.N.Y. 2016) ("Because materiality, which turns on the existence of probable cause, is a legal question, resolving whether information allegedly omitted from a search warrant application was material does not require an evidentiary hearing.").

3. Particularity and Overbreadth

The particularity requirement of the Fourth Amendment "guards against general searches that leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized." *United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990). The requirement is directed at ensuring that the warrant enables "the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize." *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992).

> [C]ourts may tolerate some ambiguity in the warrant so long as "law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant."

United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013) (quoting *United States v. Young*, 745 F.2d 733, 759 (2d Cir. 1984)).

The particularity requirement consists of three essential components. "First, a warrant must identify the specific offense for which the police have established probable cause." *Galpin*, 720 F.3d at 445. Second, the warrant must describe the place to be searched. *Id.* at 446. Finally, the warrant must "specify the items to be seized by their relation to designated crimes." *Id.*

Those categories of evidence particularly described in a warrant must also be supported by probable cause to ensure that the warrant is not overly broad. Thus, "[a]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based." *Id.* (internal quotation marks

omitted); *see United States v. Lustyik*, 57 F. Supp. 3d 213, 228 (S.D.N.Y. 2014) ("[T]he overbreadth inquiry asks whether the warrant authorized the search and seizure of items as to which there was no probable cause." (internal quotation marks omitted)).

C. Discussion

1. The Covert Affidavit Was Not Misleading

The vast majority of the statements in the Covert Affidavit that Schulte claims are misrepresentations are, in fact, true, and, as a result, do not support suppression. *See United States v. Lahey*, 967 F. Supp. 2d 698, 716 (S.D.N.Y. 2013) (*Franks* relief not warranted because the defendant "failed to prove that [the challenged paragraph] even contains a misrepresentation or an omission"); *United States v. Tufaro*, 593 F. Supp. 476, 483 (S.D.N.Y. 1983) (same).

First, Schulte's assertion that Agent Donaldson's statement that the Classified Information "appears to have been stolen from the CIA Component sometime between the night of March 7, 2016 and the night of March 8, 2016," is false ignores the actual language of the Affidavit. (*See* Ex. A ¶¶ 8(c), 10, & 13). In assessing that the Classified Information "appears" to have been stolen between March 7 and 8, 2016, Agent Donaldson described the methodology used to arrive at that conclusion—namely a comparison of dates of the records in the Classified Information with data stored on the LAN—but cautioned that that assessment was "preliminary," *i.e.*, subject to change. Agent Donaldson also stated that despite the FBI's "preliminary" assessment, it was also possible that the Classified Information was stolen later (*see id.* n.1), which tracks the information provided in the Disclosure Letter that the Classified Information was actually stolen in April 2016. Agent Donaldson accurately described the state of the investigation: Based on the analysis done to that point, it appeared that the Classified Information was stolen between March 7 and 8, a time-period

during which Schulte had an opportunity to steal the Classified Information without detection, but that further investigation could show that the Classified Information was stolen later.

Schulte entirely ignores Agent Donaldson's cautionary language, arguing instead that (i) in the Disclosure Letter, the Government stated that Schulte took the Classified Information in April 2016 (rather than between March 7 and 8, 2016); and (ii) a CIA analyst (the "Analyst") stated that the March 7 timestamp analysis was incorrect. Schulte's criticism misses the mark, however, because none of this information was available to Agent Donaldson before he swore out the Covert Affidavit. *Maryland v. Garrison*, 480 U.S. 79, 85 (1987) ("Those items of evidence that emerge after the warrant is issued have no bearing on whether or not a warrant was validly issued.").

For example, the FBI's conclusion that Schulte stole the Classified Information in April 2016 is based on a review of *all* of the Classified Information disclosed by WikiLeaks, not just the data that was disclosed in the March 7 Leak, as well as a review of a tremendous volume of forensic material at the CIA. WikiLeaks made 25 disclosures containing CIA data after the date of the Covert Affidavit. Those subsequent disclosures showed, among other things, that the Classified Information contained materials created in different places and stored in different files on the LAN, facts that are critical to determining from where, how, and when the Classified Information was stolen. Moreover, as of the date of the Covert Affidavit, and as that affidavit made clear, the FBI was "continuing to review an enormous volume of electronic evidence" from the CIA (Ex. A ¶ 39), which shed light on how the Classified Information was stolen.

Similarly, the interview of the Analyst confirms that the CIA's initial assessment, like the FBI's, was that the Classified Information was stolen between March 7 and 8, 2016. (*See* Shroff C. Decl., Ex. I). But the interview also shows that it was not until March 22, 2017, more than a week after the date of the Covert Affidavit, that the Analyst reported to the FBI that additional

investigation had contradicted that initial assessment. Agent Donaldson could not have known on March 13, of course, that subsequent investigation would reveal the timing analysis in the Covert Affidavit was wrong, but he nevertheless guarded against that possibility by alerting the magistrate judge to the "preliminary" nature of the timing analysis in the Covert Affidavit and acknowledging that the Classified Information could have been stolen later. By demanding suppression based on information in the Disclosure Letter and the Analyst's interview, Schulte asks the Court not to impose a standard of honesty on the FBI, but rather one of clairvoyance.

Second, Schulte argues that Agent Donaldson's assessment that the Classified Information was "likely" stolen from the back-up files housed on the Back-Up Server was false. Again, Schulte ignores the actual contents of the Covert Affidavit. Looking at the entirety of the Affidavit, Agent Donaldson set forth several facts that establish that Schulte likely stole the Classified Information, including that Schulte was a disgruntled employee who had illegally manipulated CIA computer systems in the past to gain unauthorized access to sensitive CIA material, flouted CIA security protocols, displayed a guilty conscience, and planned to leave the country shortly after the March 7 Leak. Agent Donaldson also described how Schulte was one of a few CIA employees who had access to the Classified Information through the Back-Up Server. Against this backdrop—in which Schulte was a prime suspect and had access to the Back-Up Server—Agent Donaldson expressed his assessment that it was "likely" that the Classified Information came from the Back-up Server because (i) data was backed up daily to the back-up files on the Back-Up Server; (ii) the resulting back-up files contained a "snapshot" of the data on the LAN from each day; (iii) the back-up file thus contained multiple iterations of the same or similar data; (iv) the Classified Information similarly contained multiple iterations of the same or similar data; and (v) individuals familiar with the LAN stated that it was "difficult, if not impossible" to copy these different iterations from any

place on the LAN other than the Back-Up Server. (Ex. A ¶ 10). Considering all of these facts together, and in light of Agent Donaldson's years of experience doing national security investigations, his assessment that the Classified Information was "likely" stolen from the Back-Up Server should be credited. *See United States v. Saipov,* 17 Cr. 722 (VSB), Dkt. # 189 (S.D.N.Y. July 11, 2019) ("The experience of the law enforcement agents involved in preparing the warrant application is particularly relevant to the analysis, as 'experience and training may allow a law enforcement officer to discern probable cause from facts and circumstances where a layman might not.'" (quoting *Gaskin,* 364 F.3d at 457)); *United States v. Delossantos*, 536 F.3d 155, 161 (2d Cir. 2008) (same); *United States v. Fama*, 758 F.2d 834, 838 (2d Cir. 1985) (same).

Schulte does not challenge that the Classified Information was taken from a back-up file, but instead argues that the back-up files were also stored at an offsite location (the "Offsite Server"), based on a network diagram of the LAN, and that, in one CIA Group contractor's opinion, the "easiest" way to steal those back-up files was from the Offsite Server. None of this information, however, renders Agent Donaldson's assessment misleading. Initially, while it is true that the back-up files were also stored in an Offsite Server, Agent Donaldson never suggested that the only place that the back-up files existed was the Back-up Server. Nor did Agent Donaldson opine in the abstract on the easiest method of exfiltrating the Classified Information from the LAN. Rather, he merely stated that it was "likely" that the Classified Information had come from the Back-Up Server, an eminently reasonable conclusion, given that the Back-Up Server contained the back-up files that mirrored the Classified Information, and Schulte—whom the FBI properly identified as a likely perpetrator of the theft—had access to it. *Gates*, 462 U.S. at 230-31 (courts do not isolate each factor of suspicion but look at the totality of the circumstances). The opinion of the contractor—who did not have access to all of the information and who had no relevant

investigatory experience—in no way undermines that assessment, particularly when (i) that opinion is contradicted by [redacted], a LAN system administrator and a witness *upon whom Schulte relies in his motion*, who stated that "the easiest way to steal the data leaked by WikiLeaks" was for someone with administrative access to the LAN to "simply remov[e] the back-up file from the network application" (*i.e.*, the Back-Up Server) (Shroff C. Decl., Ex. I); and (ii) even if the contractor's opinion was relevant, it was not conveyed to the FBI until February 2018, nearly a year after the date of the Covert Affidavit, *see Garrison*, 480 U.S. at 85.

Third, Schulte also claims that Agent Donaldson misstated how the back-up files were created by describing it as an "automated process," because, in the Disclosure Letter, the Government noted that this "automated process" had to be "manually initiated." An "automated process" is still "automated," however, even though a person has to initiate it; an ATM—or "Automated Teller Machine"—is no less "automated" simply because a person has to enter a debit or credit card and command prompts. So too with the LAN's back-up process—even though a person had to start the process, it nevertheless was automatically completed, and thus was "automated." Schulte's argument is nothing more than semantic quibbling.

Fourth, Schulte argues that Agent Donaldson was wrong when he stated that "less than 200 people had access to the CIA Group's LAN on which the Classified Information was stored." (Ex. A ¶ 9). Schulte does not dispute that the CIA Group was responsible for using and maintaining the LAN, that as of March 2016 fewer than 200 employees were assigned to the CIA Group, or that only these employees had access to the LAN. (*See id.* ¶ 8(b)). Rather, Schulte argues that Agent Donaldson failed to note in the Covert Affidavit that a second CIA group ("CIA Group-2"), [redacted], allegedly also had access to the LAN. The reason for that omission is simple—Schulte's assertions about CIA Group-2's access to the

LAN are untrue. [redacted] In short, Schulte is simply wrong.

To the extent Schulte argues that [redacted] security measures could have been or were breached by a CIA Group-2 employee, Schulte has pointed to no evidence in support of that claim or that shows Agent Donaldson was aware of any such evidence when he swore to the Covert Affidavit. *Franks*, 438 U.S. at 171 (defendant must provide "statement of supporting reasons," together with supporting affidavits or witness statements). [redacted] Schulte has, of course, failed to submit an affidavit attesting to those facts, which are presumably within his personal knowledge given that he was a LAN administrator. *United States v. Barrios*, 210 F.3d 355 (2d Cir. 2000) (no evidentiary hearing required regarding a motion to suppress evidence from a search where the defendant failed, among other things, to submit an affidavit from "someone alleging personal knowledge of the relevant facts"). In any event, Agent Donaldson did note that an "employee lacking System Administrator access could, at least theoretically, gain access to the Back-Up Server by finding a 'back-door'

into the Back-up Server," (Ex. A ¶ 11(b) n.4), thus flagging for the magistrate judge that any number of CIA employees could have accessed the Back-Up Server without authorization.

Fifth, Schulte contests Agent Donaldson's statement that one had to be a System Administrator to access the back-up files on the Back-Up Server. (*Id.* ¶ 11). Schulte's argument is based on a distorted reading of the Covert Affidavit. Agent Donaldson said that System Administrators were a limited group of employees—of which Schulte was one—who had been given access to the Back-Up Server. Schulte does not dispute that statement, but claims that there were means through which non-System Administrators could have stolen the back-up files from the LAN, citing to [redacted] Setting aside that this interview occurred a month *after* the date of the Covert Affidavit and thus is irrelevant to the motion, *see Garrison*, 480 U.S. at 85, the Covert Affidavit is entirely consistent with [redacted] statement. Agent Donaldson stated in the Covert Affidavit that "[i]t is, of course, possible that an employee who was not designated Systems Administrator could find a way to gain access to the Back-Up Server," and gave two examples of ways that could happen (Ex. A ¶ 11(b) n.4), thus notifying the magistrate judge that an employee without System Administrator access could have stolen the back-up files, *i.e.*, the very information Schulte claims Agent Donaldson withheld.

Sixth, Schulte argues that Agent Donaldson was misleading by stating that WikiLeaks disclosed other System Administrator's names or pseudonyms, but not Schulte's, because in one of the Leaks, WikiLeaks disclosed Schulte's username, "SchulJo." Schulte's claim bizarrely equates a person's username with their actual name. Agent Donaldson did not refer to Schulte's

username in the Covert Affidavit; he stated only that Schulte's *name* did not appear in the initial Leak, which is true. Simply put, the public would have no idea that "SchulJo" was Joshua Schulte.

Schulte's argument fails for a second and equally fatal reason, which is highlighted by Schulte's dismissive claim that a simple "text search" would have shown that Schulte's username appeared in the Classified Information. That is true, but that same text search would also show that Schulte's username does not appear until a disclosure dated March 31, 2017, *i.e.*, two weeks after the date of the Covert Affidavit.[6] *See Garrison*, 480 U.S. at 85. Schulte's criticism is essentially that Agent Donaldson failed to see the future.

2. Any Errors Were Not Material

Schulte's motion fails for the additional reason that none of the alleged errors in the Covert Affidavit is material. To determine whether the purported errors in the Covert Affidavit are material, the Court should disregard the alleged false statements and add in any allegedly damaging omitted information and determine whether the affidavit nevertheless contains probable cause for the search. *See Awadallah*, 349 F.3d at 64. Here, even without the statements that Schulte claims are inaccurate, the Covert Affidavit still lays out, at a minimum, Schulte's access to the Classified Information, his motive to harm the CIA, his willingness to manipulate the CIA's computer system and its access controls, and his consciousness of guilt. Those facts are more than enough to support probable cause and thus, Schulte's motion should be rejected. *See Klump*, 536 F.3d at 119.

---

[6] If a user manipulates the March 7 Leak, the user can see Schulte's username. Specifically, one part of that disclosure contains multiple versions of a certain file. Some but not all of those versions display a hyperlink that, if a user hovers a mouse pointer over the link, shows a file path that includes Schulte's username as part of the file path. Other versions show that Schulte's username was redacted by WikiLeaks. Thus, in order to view Schulte's username, one would have to: (i) navigate to the specific file where the username appears; (ii) navigate to the specific version of that file where the username appears and is not redacted; and (iii) hover over the correct hyperlink so that the username is visible. Screenshots of this effect are attached as Classified Exhibit K. These instances of Schulte's username do not appear in response to a word search.

As described in the preceding section, much of what Schulte claims to be false in the Covert Affidavit is plainly true. The only actual errors in the Covert Affidavit are (i) Schulte was an administrator for the specific part of the Back-up Server that contained the back-up files, instead of the entire Back-Up Server; (ii) Schulte was one of at least five such administrators, as opposed to three; and (iii) Schulte's illegal restoration of his administrative privileges occurred with respect to a different CIA program than the one described in the Covert Affidavit and happened on or about April 14, 2016, instead of April 11, as stated in the Affidavit. Correcting these errors, however, does not undermine the probable cause in the Covert Affidavit.

First, though Schulte was an administrator for only part of the Back-Up Server, as opposed to the Back-Up Server as a whole, he was the administrator for the part of the Back-Up Server that housed the back-up files from where the Classified Information was likely stolen, meaning that he still had access to the stolen data. *Second*, that Schulte was one of at least five employees, as opposed to three, with authorized access to that specific part of the Back-Up Server does not change that Schulte was one of a small pool of CIA employees with that type of access. *Third*, regardless of the specific program to which Schulte restored his access, or when he did so, the fact remains that Schulte manipulated CIA computer systems without authorization to gain access to sensitive CIA material. Even as corrected, these facts continue to show that Schulte was a rogue CIA employee with the opportunity to steal the Classified Information.

While these facts, standing alone, may be sufficient for probable cause, the Covert Affidavit contains much more support, describing how Schulte (i) had a motive to harm the CIA because he was angry at how the CIA had handled his complaint against a colleague, to the point that Schulte threatened to go to the media (Ex. A ¶¶ 17-18); (ii) secured unauthorized access to a CIA project in a deceitful manner again in May 2016 and then promptly used that access to harm

the CIA by preventing other employees from working on the project (*see id.* ¶ 15(c)); (iii) flouted CIA security protocols by connecting removable media to the LAN and by removing a document from the CIA, despite being told not to (*see id.* ¶¶ 17 & 19(c)); (iv) drafted a purported "resignation email," in which he claimed essentially that he had warned CIA management about security concerns with the LAN[7] that were so significant that the LAN's contents could be posted online—precisely what happened four months later (*see id.* ¶ 19); and (v) demonstrated a guilty conscience, specifically through his persistent inquiries to his former colleagues about the investigation on the day of the initial Leak (including his suspicion that he was a target of the investigation) and his travel out of the country (for only the second time) shortly after the initial Leak (*see id.* ¶¶ 20-21). When combined with the corrected facts describing Schulte's access and illegal activity on the LAN in April 2016, these facts are more than sufficient to establish probable cause.

Schulte does not challenge the truth of these assertions in his motion, but instead argues that there are innocent explanations for these actions. (*See* Res. Br. 19). "The fact that an innocent explanation may be consistent with the facts alleged . . . does not negate probable cause." *Klump*, 536 F.3d at 120 (citation omitted). Moreover, Schulte's explanations do not make these facts any less suspicious. For example, while it is true that Schulte lost his access to a CIA project because he was moved to another part of the CIA Group, that does not explain why Schulte then illegally restored his access to that project. Schulte also claims that the fact that he was upset at the Agency when he left does not play into probable cause, but of course, those facts demonstrate a motive to harm the Agency. Finally, Schulte claims that his intense interest in the investigation following the initial Leak was not suspicious because he was employed by the CIA Group, but that does not explain why Schulte would believe *he* was a target of the investigation. Even as corrected, the

[7] There is no record of Schulte reporting any such security concerns to CIA management.

Covert Affidavit establishes probable cause, and thus, the errors are not material. *See, e.g.*, *Lahey*, 967 F. Supp. 2d at 712 (finding alleged misrepresentations immaterial because even without them, the remaining allegations established probable cause that defendant engaged in criminal activity).

Furthermore, rewriting the Covert Affidavit to fully incorporate Schulte's purported deficiencies would not support suppression because it would not change the aforementioned facts. While stripping out the timing analysis in the Covert Affidavit and all the facts showing how Schulte essentially had unmonitored access to the LAN on March 8, 2016 eliminates one particularly ripe opportunity for Schulte to have stolen the Classified Information, it remains true that Schulte had access to the Classified Information, and thus the chance to steal it, at other points as well. Similarly, inserting the facts that Schulte claims were improperly omitted—namely that a contractor believed that it was easier to steal the Classified Information from the Offsite Server, that an employee without Schulte's level of access could have stolen the Classified Information, that the back-up process was not fully automated, or that WikiLeaks also (at some later date) disclosed Schulte's username—would not change the facts establishing Schulte's complicity, including his motive, access to the Classified Information, disregard for CIA's security protocols, illegal manipulation of the CIA's computer systems, and demonstration of a guilty conscience.

Thus, even if the Covert Affidavit was rewritten to Schulte's (incorrect) specifications, it would still establish probable cause by showing that Schulte was a CIA employee with a grudge against the CIA and a track record of improperly accessing and taking classified information, who left the CIA claiming that classified information from the LAN would one day be sprayed across the Internet and who worried about the investigation when his "prophecy" came to pass. The corrected Covert Affidavit thus provides overwhelming evidence of Schulte's guilt, including evidence which has no innocent explanation, and thus stands in stark contrast to the affidavits

found lacking in the cases relied upon by Schulte. *See United States v. Reilly*, 76 F.3d 1271, 1279 (2d Cir. 1996) (good faith exception did not apply where warrant failed to disclose information about the property on which the defendant was growing marijuana plants, which was relevant to curtilage issue); *Lahey*, 967 F. Supp. 2d at 724 (omitted information specifically showed that activity in which defendant was engaged was innocent); *United States v. Padilla*, 986 F. Supp. 163, 168 (S.D.N.Y. 1997) ("bulk" of complaint was wrong, and remaining information was simply that defendant drove another person to a narcotics transaction); *United States v. Big Apple Bag Co.*, 306 F. Supp. 2d 331, 334 (E.D.N.Y. 2004) (affiant claimed to see "thousands" of items used for narcotics trafficking when in fact the affiant saw only three); *United States v. Roman*, 311 F. Supp. 3d 427, 439 (D. Mass 2018) (affidavit claimed that narcotics transaction occurred at defendant's property, when illegal transaction actually occurred at source's business).

3. Any Errors Were Not Deliberate

Even assuming *arguendo* that the Covert Affidavit contains material misrepresentations or omissions, Schulte fails to make a "substantial preliminary showing" that these purported errors were deliberate or recklessly made, as he must to prevail on his motion, or even to secure a hearing. *See Falso*, 544 F.3d at 134. To be clear, Schulte does not offer a single fact that shows that the agents who conducted this investigation intentionally misstated anything in the Covert Affidavit. Instead, he claims that these "errors" must have been deliberate or at least reckless because, according to him, the errors all "'dr[o]ve in the same direction: establishing a connection' between Mr. Schulte and the theft of classified information, 'which connection the fuller evidence did not support.'" (*See* Res. Br. 20-21 (quoting *Lahey*, 967 F. Supp. 2d at 723)). Schulte is wrong.

In the short period of time between the initial Leak and the execution of the Covert Affidavit, the FBI had already amassed a substantial volume of evidence that Schulte was the

perpetrator, more than justifying the FBI's need to obtain a warrant to search his home. *See supra* pp. 7-15. Moreover, given the gravity of the Leaks, there was tremendous urgency to find the leaker, to attempt to stop further unlawful dissemination, and to determine what had already been transmitted to WikiLeaks and thus mitigate the significant national security harm already caused. Accordingly, the FBI could not wait for the investigation to unfold fully before acting.

To be sure, as the investigation developed, the FBI obtained information that some of the statements in the Covert Affidavit were incorrect, albeit in immaterial ways. *See supra* pp. 28-31. The caution and candor displayed by Agent Donaldson in the Covert Affidavit, however, undercuts any contention that there was a deliberate intention to mislead the magistrate judge. In the Covert Affidavit, Agent Donaldson made clear to the magistrate judge that the FBI's assessments at the time were preliminary and subject to change. (Ex. A ¶ 8(c)(i)). With respect to the timing of the theft, Agent Donaldson laid out the facts that led to his "preliminary" view that the Classified Information was stolen between March 7 and 8, 2016, and went on to note that on March 8, Schulte had a particularly ripe opportunity to steal the Classified Information. (*Id.*). But Agent Donaldson also made sure to disclose the fact that the data could have been taken on a later date as well (*id.* ¶ 8(c)(iii) n.1), which would render Schulte's opportunity on March 8 irrelevant. Similarly, Agent Donaldson explained how System Administrators like Schulte had specialized access to the Back-Up Server, but noted that it was only "likely" that the Classified Information had been stolen from the Back-Up Server (*id.* ¶¶ 10-11), and that, in any event, a non-System Administrator could have stolen the data as well (*id.* ¶¶ 10(d) n.3). Moreover, Agent Donaldson, in reporting Schulte's colleagues' views of Schulte, went out of his way to note that some of Schulte's colleagues thought he was trustworthy and that some of his colleagues did not report any concerns about Schulte's security practices. (*Id.* ¶ 18). Even crediting Schulte's breathless description of the purported

significance of the "errors" in the Covert Affidavit, Agent Donaldson's determined effort to ensure that the magistrate judge knew the whole truth is inconsistent with the requisite subjective intent to mislead. *See Rajaratnam*, 719 F.3d at 154 (defendant must show affiant had the subjective intent to mislead and not simply that affiant omitted "critical" information or information that a reasonable person would have included).

None of the cases upon which Schulte relies supports his argument that Agent Donaldson deliberately tried to mislead the magistrate judge or recklessly disregarded the truth. In *Reilly*, 76 F.3d at 1280, the Second Circuit found that the good faith exception did not apply because the officer's description of the land to be searched was "calculated to mislead." Here, it is simply implausible that Agent Donaldson made a "calculated" decision to deceive the magistrate judge, but still described facts that could undercut the probable cause. *See supra* pp. 7-15. In *Lahey*, the court found that the affiant recklessly made misrepresentations because the misrepresentations led to the conclusion that the full record belied. *See* 967 F. Supp. 2d at 722. Here, even crediting the purported misrepresentations or omissions Schulte claims, the remainder of the evidence is clearly consistent with Schulte's guilt and easily supports probable cause to search the Residence. *See supra* pp. 27-31. And in *Roman*, the court found that the affidavit omitted the "foundational piece of evidence" that "undermined the purported link between [the place to be searched] and [the criminal activity]." *See* 311 F. Supp. 3d at 441. Here, none of the purported errors or omissions about which Schulte complains can be fairly described a "foundational"—in fact, they are, at best, marginal. *See supra* pp. 27-31. Schulte is not entitled to a hearing, let alone suppression.

4. The Covert Warrant Was Not Overbroad

Schulte also argues that the Covert Affidavit was insufficient to establish probable cause to search his home, but that argument also fails.

First, Schulte's contention that the Covert Affidavit does not establish a nexus to search his home is meritless. Initially, Schulte's motion erroneously claims that the Covert Affidavit does not specify how the FBI believed that Schulte stole the Classified Information. (*See* Res. Br. 25). The Affidavit says clearly that Schulte likely stole the Classified Information "by using sophisticated computer skills to exfiltrate a substantial amount of data onto a *removable drive* and then covertly removed that drive from the CIA." (Ex. A ¶¶ 37(a)-(b) (emphasis added)). Moreover, other facts set forth in the Affidavit also show that Schulte had to use some sort of electronic media to steal the Classified Information: (i) the Classified Information was stored on the LAN in an electronic form; (ii) the LAN was "air-gapped," meaning Schulte most likely could not have transferred it from the LAN over the Internet; and (iii) the volume of the Classified Information—thousands of documents in the initial Leak alone—was so substantial that it would make no sense for Schulte to have removed it in hardcopy. Moreover, Agent Donaldson also noted that, based on his training and experience accrued over seven years in counterespionage investigations, he had learned that individuals who stole and transmitted classified information often did so using electronic devices, and that they often maintained those electronic devices in their homes. (*Id.* ¶ 22). Combining Agent Donaldson's reasoned conclusions with his statements about the nature of the LAN, the likely method of exfiltration, Schulte's illegal manipulation of CIA computer systems, Schulte's lax security practices, and the fact that he had removed CIA information improperly in the past, the Covert Affidavit certainly sets forth probable cause to search Schulte's home for electronic media and other evidence of the theft and transmittal of the Classified Information. *United States v. Cruz*, 785 F.2d 399, 405 (2d Cir. 1985) (evidence that defendant was engaged in drug trafficking, combined with agent's opinion that drug traffickers "customarily" keep evidence of their drug trafficking in their homes, established probable cause

to search defendant's home); *United States v. Benevento*, 836 F.2d 60, 70 (2d Cir. 1987) (same), *abrogated on other grounds by United States v. Indelicato*, 865 F.2d 1370 (2d Cir. 1989).

Schulte further argues that the Covert Affidavit does not assert that Schulte personally owned or possessed a computer or electronic device on which to store the Classified Information. (*See* Res. Br. 25-26). That argument, however, is a red herring. The issue is not whether Schulte owned a computer or thumb drive in March 2016 or March 2017, but rather whether there was probable cause to believe that Schulte possessed an electronic device that stored the Classified Information. As described above, the Covert Affidavit plainly set forth probable cause to believe that Schulte took the Classified Information by copying it to removable media that he smuggled out of the CIA, that Schulte had access to removable media while at the CIA, and that Schulte had no compunction about connecting that media to the LAN, even if barred by CIA security protocols (Ex. A ¶ 19(c) (describing some of Schulte's colleagues' concerns that Schulte would disregard CIA protocols with respect to "when and what kinds of media or data (such as external drives) could be connected or uploaded to the CIA computer systems")).

Second, contrary to Schulte's staleness argument, there was certainly probable cause to believe that Schulte might still have the Classified Information in electronic form as of March 13, 2017, when Agent Donaldson submitted the Covert Affidavit. When Schulte left the CIA in November 2016, he was angry at the agency, and WikiLeaks had not yet disclosed any of the Classified Information. Indeed, WikiLeaks' first disclosure of the Classified Information did not come until March 7, 2017, just days before the Covert Affidavit was submitted. Thus, although the FBI believed initially that Schulte had stolen the Classified Information in March 2016, the evidence available at the time still reasonably supported an inference that Schulte had provided the Classified Information to WikiLeaks as recently as March 7, 2017. Thus, the FBI reasonably

could have inferred that Schulte had passed classified information to WikiLeaks within the week prior to obtaining the Covert Warrant, and might continue to possess classified information. *See United States v. Ortiz*, 143 F.3d 728, 732 (2d Cir. 1998) (if affidavit shows "continuing conduct or an ongoing activity," then "the passage of time between the last described act and the presentation of the application becomes less significant."); *Singh*, 390 F.3d at 183 (same).

Schulte asserts that because the Government's theory now is that Schulte transmitted the Classified Information in late April or early May 2016, that shows that there was no reason to believe that his home would still contain evidence of the crime. (Res. Br. 30 n.6). But Schulte's argument proves too much: The evidence that allowed the Government to determine when Schulte transmitted the Classified Information was found, among other places, in Schulte's home and Google account, which was obviously obtained only after the Covert Affidavit was executed. (*See* Ex. E ¶¶ 27-28 (explaining how FBI found multiple hard drives in Schulte's apartment and searches in his Google account conducted between April 30 and May 1, 2016 for tools to securely erase those brands of hard drives and to verify that a large file had been transferred)). Moreover, even given Schulte's expertise, the FBI might still have been able to recover evidence he had tried to delete. (*See* Ex. A ¶ 27 (describing how forensic tools could potentially recover deleted data)).

Indeed, even if the FBI could have determined only that Schulte had deleted or destroyed material, that would still be evidence. For example, the fact that Schulte tried to delete a file related to one of the CIA cyber-tools disclosed in the Leaks from electronic media found in his home (which he did) or tried to shred CIA documents (which he also did) would be relevant evidence of the theft of the Classified Information. *See, e.g.*, *United States v. Robinson*, 635 F.2d 981, 986 (2d Cir. 1980) (evidence that defendant tried to destroy passport was admissible as evidence of consciousness of guilt). That is a far cry from the authority Schulte relies on, which does not

involve potential ongoing conduct or material that could constitute evidence even if deleted. *See United States v. Griffith*, 867 F.3d 1265, 1275 (D.C. Cir. 2017) (probable cause to search residence for defendant's home was stale when the crime had occurred a year before the search and the defendant had been incarcerated for 10 months during that period); *United States v. Paul*, 692 F. Supp. 186, 193 (S.D.N.Y. 1988) (search warrant allegations were stale when they pertained to two isolated bribes that occurred five months before the search).

II. THE CHILD PORNOGRAPHY EVIDENCE SHOULD NOT BE SUPPRESSED

Schulte next contends that the Supplemental Warrants, which among other things authorized the seizure of child pornography on the Electronic Devices, are invalid because the affidavits supporting those warrants deliberately or recklessly omitted materials facts. As a result, Schulte argues that the Court should "suppress the resulting evidence." (Res. Br. 40).[8] As described below, Schulte has failed to carry his "heavy" burden to show that the affidavits in question omitted material facts or that those omissions were designed to mislead the issuing judges. In any event, the Court need not reach the *Franks* issue at all. Whether or not the Government obtained the Supplemental Warrants, the Government inevitably would have discovered the child pornography in plain sight during the previously authorized search of the Electronic Devices for the Espionage Offenses. As a result, Schulte's motion should be denied without a hearing.

[8] Schulte does not challenge the portions of the Supplemental Warrants authorizing the search of the Electronic Devices for evidence of the copyright infringement offenses. As a result, regardless of the outcome of this motion, the portion of the Supplemental Warrants relating to the copyright infringement offenses remains valid and any evidence recovered pursuant to that portion of the warrants should not be suppressed. *See, e.g.*, *George*, 975 F.2d at 79 ("Fourth Amendment guarantees are adequately protected by suppressing only those items whose seizure is justified solely on the basis of the constitutionally infirm portion of the warrant, which no reasonably well-trained officer could presume to be valid.").

A. Schulte's Motion Fails At Both Stages of the *Frank's* Analysis

1. Relevant Facts

Schulte's motion challenges warrants executed on April 14 and May 10, 2017 in the Eastern District of Virginia, which together constitute the Supplemental Warrants (the "April 2017 Warrant" and "May 2017 Warrant"). In those warrants, which are nearly identical, the FBI sought and obtained authorization to expand the scope of the search of the Electronic Devices to include evidence of child pornography and copyright infringement offenses.

In support of its application for the April 2017 Warrant, the Government submitted an affidavit by FBI Special Agent Richard J. Evanchec, an agent experienced in counterespionage investigations and the use of computers more generally in criminal activity (the "April Affidavit"). (Ex. C ¶ 1). Initially in the April Affidavit, Agent Evanchec explained that the Government was already searching the Electronic Devices for evidence of the Espionage Offenses pursuant to a search warrant, and he attached and incorporated by reference the Covert Affidavit and Warrant. (*Id.* ¶ 2-4, 11-12 & n.2). He then stated that while searching the Electronic Devices for evidence of the Espionage Offenses, the FBI had discovered evidence of child pornography and copyright offenses. (*Id.* ¶¶ 3-4). Upon discovery of that evidence, the FBI "promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek additional" authorization to search the Electronic Devices for evidence of child pornography and copyright infringement offenses. (*Id.* ¶¶ 3-4, 6).[9]

[9] The FBI, in consultation with the U.S. Attorney's Office, had stopped searching the Electronic Devices after discovering evidence of child pornography and copyright infringement on the Desktop Computer and resumed those searches upon obtaining the April 2017 Warrant. (*See* Classified Ex. L (Email from Agent Evanchec)).

Agent Evanchec learned from FBI members searching the Electronic Devices, that on or about April 7, 2017, "a photograph was discovered on Schulte's desktop computer (the 'Desktop Computer') that appears to depict child pornography" (the "CP Image," attached as Exhibit O). (*Id.* ¶ 13). The CP Image appears to depict "a naked young child on all fours and what appear to be two adults around her, one of whom appears to be performing a sexual act on the child." (*Id.* ¶ 14). Notably, Agent Evanchec stated that "it is possible that the CP [Image] . . . could be altered and not [be] a real picture." (*Id.* ¶ 14 n.5). Nevertheless, Agent Evanchec had "viewed the CP [Image] on the Desktop Computer and believe[d] that it is an actual photograph." (*Id.*).[10]

Agent Evanchec then explained how individuals involved in child pornography offenses use electronic devices to facilitate their crimes, including that they often (i) collect and distribute child pornography on various devices such as the Electronic Devices; (ii) back up or transfer files from their older computers' hard drives to that of their new computers, so as not to lose relevant data; and (iii) store files related to their criminal activity to other storage media. (*Id.* ¶¶ 16-17).

With respect to the CP Image, Agent Evanchec stated that it "was likely downloaded via the Internet using the Desktop Computer or other of the [Electronic] Devices." (*Id.* ¶ 18). As a result, the Electronic Devices "may contain messages, emails, photographs, and/or videos relating to the possession, receipt, or production of child pornography." (*Id.*). Agent Evanchec also explained that files containing child pornography, like the CP Image, may reside on the Electronic Devices even after they are deleted. (*Id.*). For example, deleted files may "reside in 'slack space' (space that is not being used for storage of a file) for long periods of time before they are

[10] Agent Evanchec also discussed his review of Schulte's Google searches, which were obtained pursuant to a search warrant (the "CP Google Searches"). In particular, he stated that on a number of occasions in or about 2011 and 2012, Schulte appeared to have searched the Internet for child pornography, and Agent Evanchec provided examples of those searches. (Ex. C ¶ 15).

overwritten" and a computer's operating system may keep data related to deleted files in a "'swap' or 'recovery' file." (*Id.*). In the same paragraph in which Agent Evanchec stated that the CP Image was likely downloaded via the Internet, he stated that files viewed on the Internet are generally automatically downloaded onto a specific location on a computer:

> [F]iles that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or 'cache.' The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

(*Id.*).

Based on the foregoing, Agent Evanchec sought authorization to search the Electronic Devices for evidence of child pornography offenses. (*Id.* ¶¶ 19-20). Through the April Affidavit, Agent Evanchec also sought and obtained authorization to search the Electronic Devices for evidence of copyright infringement offenses. Notably, the search of the Electronic Devices for evidence of the child pornography and copyright infringement offenses was to be conducted pursuant to the same procedures as those set forth in the Covert Search Warrant. (*Id.* ¶¶ 20, 29).

On May 10, 2017, the FBI executed the May 2017 Warrant. The affidavit in support of the May 2017 Warrant, which was submitted by FBI Special Agent Garrett Igo, was nearly identical to the April Affidavit except that it omitted the paragraph discussing the CP Google Searches (the "May Affidavit"). In lieu of that paragraph, Agent Igo included a footnote noting that the Government had previously executed the April 2017 Warrant relying on the CP Google Searches. (Ex. D ¶ 14 n.6). Agent Igo explained that the CP Google Searches were obtained by conducting searches for child pornography through evidence obtained from Google pursuant to a warrant related to the Espionage Offenses, prior to obtaining the April 2017 Warrant. (*Id.*) As a result,

"out of an abundance of caution, and because the search of the [Electronic] Devices (which consists of numerous terabytes of data) [was] only partially complete," Agent Igo submitted the May Affidavit, which did not rely in any way on the CP Google Searches. (*Id.*). Agent Igo also stated that agents were instructed "to stop any searches related to the CP Offenses absent renewed additional authorization under Rule 41 of the Federal Rules of Criminal Procedure." (*Id.*).

2. Discussion

a. The Alleged Omissions Were Not Material

Schulte contends that the April and May Affidavits should have included that (i) the CP Image was found in the Desktop Computer's page file, an area of the computer that is "generally" not accessible to the computer's user (Res. Br. 36); (ii) there was limited metadata associated with the image such that it "may have been residing in the page file" for a long period of time (*id.*; Bellovin Decl. ¶ 11); and (iii) about 20% of the image was blacked out, potentially supporting the conclusion that the image was automatically downloaded to the Desktop Computer (Res. Br. 34). None of this information undercuts probable cause.

Contrary to Schulte's apparent view, the materiality component is not satisfied by demonstrating the mere relevance of information omitted from a warrant application. Rather, under *Franks*, materiality depends on whether the omitted information was "necessary to the finding of probable cause," *Franks*, 438 U.S. at 156, and not on what might have been relevant to that finding, let alone of potential interest to a magistrate judge. *See Colkley*, 899 F.2d at 301.

Here, the omitted information simply presented the *possibilities* that Schulte did not have access to the CP Image, never viewed it, and that the Image may have been stored on the Desktop Computer for a long period of time. But an omitted fact is not material under *Franks* simply because it creates some possibility of a contrary conclusion; it is material only if it would actually

defeat the effort to show probable cause. *See Salameh*, 152 F.3d at 113-14 (omission held not material where affidavit alleged that bomb-making materials were found in an apartment associated with the target, but omitted the fact that an electrical engineering professor who claimed to reside in the apartment told agents that the materials were used for his studies); *Klump*, 536 F.3d at 120 (omission held not material where affidavit stated that PVC pipe, which agents observed being carried into the premises, is often used to grow marijuana, but failed to inform court that there was ongoing construction at the premises); *United States v. Levasseur*, 816 F.2d 37, 44 (2d Cir. 1987) (omission held not material despite court's "concern" that the affidavit "seriously understated" facts calling into question the informant's reliability). That remains true even where the omitted information is sufficiently important that the affiant "should have disclosed" it. *United States v. Bianco*, 998 F.2d 1112, 1126 (2d Cir. 1993) (although the affiant "should have disclosed" a fact that detracted from the Government's need for a roving Title III order, omission was not material because there would still be a basis for the order).

Here, the possibilities proffered by Schulte would not have defeated probable cause, given the limited nature of the authorization sought through the Supplemental Warrants. At the time the agents sought those warrants, law enforcement was already authorized to search the Electronic Devices, and the only relief sought through the Supplemental Warrants was to expand the search of the Electronic Devices to include evidence of child pornography and copyright infringement.

Against this backdrop, Schulte's materiality arguments fall apart. The fact that it was *possible* that Schulte might never have viewed the CP Image or that it was automatically downloaded to the Desktop Computer is not material. As an initial matter, the affidavits contemplated that the CP Image might have been downloaded absent direct action by Schulte or anyone else, stating that the CP Image was "likely downloaded via the Internet" and that "files that

have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or 'cache.'" (Ex. C ¶ 17). Even if Schulte had visited a website that automatically distributes electronic images of child pornography and the CP Image was automatically downloaded to his Desktop Computer when he did so, that would be substantial evidence justifying the continued search of the Desktop Computer for additional evidence of child pornography. *See, e.g.*, *United States v. Bailey*, 272 F. Supp. 2d 822, 824-25 (D. Neb. 2003) ("[K]knowingly becoming a computer subscriber to a specialized internet site that frequently, obviously, unquestionably and sometimes automatically distributes electronic images of child pornography to other computer subscribers alone establishes probable cause for a search of the target subscriber's computer even though it is conceivable that the person subscribing to the child pornography site did so for innocent purposes and even though there is no direct evidence that the target subscriber actually received child pornography on his or her computer.").

Regardless, Schulte's argument in this respect is built on a false premise: that a search warrant must be based on probable cause that Schulte himself violated the law. But "[s]earch warrants are not directed at persons; they authorize the search of place[s] and the seizure of things." *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978). So long as "there is a fair probability that . . . evidence of a crime will be found in a particular place," there is probable cause to search that place, *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (quotation mark omitted), regardless of whether property's owner is suspected of committing any crime, *Gates*, 462 U.S. at 243 n.13 ("[T]he relevant inquiry is not whether particular conduct is 'innocent' or 'guilty,' but the degree of suspicion that attaches to particular types of non-criminal acts."). Here, the undisputed fact that the CP Image was on the Desktop Computer (which law enforcement was

already authorized to search pursuant to another warrant) plainly created a "fair probability" that additional evidence of child pornography would be found on the Electronic Devices.

Furthermore, the fact that it was *possible* that the CP Image may have been present on the Desktop Computer for a long period of time did not make the search warrant stale. It is questionable whether the staleness doctrine applies at all in these circumstances—that is, where law enforcement is already authorized to search a particular place and simply sought permission to seize evidence of another crime it discovered during the course of that search. In any event, when the agents sought the Supplemental Warrants, they had no information as to how long the image had been on the Desktop Computer (which remains the case to this day) and made no representation to the issuing judges concerning that issue. Informing the judges of this lack of knowledge would not have defeated probable cause. This is particularly true given that "the staleness determination [in child pornography searches] is unique because it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes." *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006). Accordingly, it is common for courts to find that probable cause to search for child pornography was not stale even when the underlying factual allegations are many months old. *See, e.g., id.* (holding 22 month-old factual allegations not stale in child pornography context); *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010) (allegations that defendant had downloaded child pornography 18 months before the search warrant issued were not too stale to establish probable cause); *United States v. Frechette*, 583 F.3d 374 (6th Cir. 2009) (allegation that defendant had purchased a membership to a child pornography website 16 months prior to the search not stale).

In this regard, the principal case on which Schulte relies—*Raymonda*, 780 F.3d 105 (Res. Br. 38-39)—is inapposite. In that case, law enforcement obtained a warrant to search a defendant's

residence based on evidence that an IP address associated with the defendant may have accessed child pornography nine months before the warrant was executed. The Second Circuit held that the warrant was invalid on staleness grounds, reasoning that because law enforcement was relying on nine-month-old evidence, law enforcement was also required to show that the defendant "accessed [the child pornography] in circumstances sufficiently deliberate or willful to suggest that he was an intentional 'collector' of child pornography." *Id.*

Here, by contrast, the Government sought the April 2017 Warrant mere days after identifying the CP Image. At that time, law enforcement had no information as to how long the image had been on the Desktop Computer. Thus, unlike in *Raymonda*, the factual allegations here were not so old that the agents were required to show that Schulte was an intentional collector of child pornography. Moreover, as noted, the agents in this case were seeking a much more limited probable cause determination through the Supplemental Warrants—that is, the authority to seize evidence of child pornography and copyright infringement offenses during the course of the already authorized search of the Electronic Devices. In *Raymonda*, 780 F.3d at 110, by contrast, the agents were seeking authorization to search the defendant's entire residence and any electronic devices found therein in the first instance, which plainly required a higher quantum of proof.

Thus, *Raymonda* does not support Schulte's claim, and Schulte has failed to demonstrate that, regardless of the potential relevance of the omitted information, it would have actually changed the probable cause determination. For the reasons set forth above, it would not have.

b. There Is No Basis to Find That the Omissions Were Made Intentionally or with a Reckless Disregard for the Truth

Schulte also has failed to show that the agents acted with the intent to mislead or with reckless disregard for the truth. Schulte incorrectly assumes that simply because the omitted

information raised the possibilities described above, it necessarily follows that the omission of this information was intentional. That is not the law:

> An affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation. However, every decision not to include certain information in the affidavit is 'intentional' insofar as it is made knowingly. If . . . this type of 'intentional' omission is all that *Franks* requires, the *Franks* intent prerequisite would be satisfied in almost every case . . . . [Rather,] *Franks* protects against omissions that are designed to mislead, or that are made in reckless disregard of whether they would mislead, the magistrate.

Awadallah, 349 F.3d at 67-68 (quoting *Colkley*, 899 F.2d at 300-01).

Here, the record does not support a finding that the alleged omissions were designed to mislead or made in reckless disregard of whether it would mislead. As the affidavits reflect, at the time the FBI sought the April 2017 Warrant, the FBI was already authorized to search the Electronic Devices, including the Desktop Computer, for evidence of the Espionage Offenses pursuant to the Covert and Overt Warrants. When during the course of that search the FBI discovered evidence of child pornography and copyright offenses, the FBI stopped searching the Electronic Devices, promptly consulted with prosecutors, and then sought the April 2017 Warrant. (Ex. L (Agent Evanchec: "We've been on a stand-down order since [April 10, 2017] on a review of some of [Schulte's] evidence because of [the discovery of evidence of child pornography and copyright infringement offenses]."). Then, after discovering that the April 2017 Warrant relied on the CP Google Searches, the FBI sought the May 2017 Warrant "out of an abundance of caution," alerting the issuing judge to the potential error.

The agents' decisions to seek the April 2017 Warrant at a time when they already had authorization to review the Electronic Devices, and then seek the May 2017 Warrant after discovering a potential error in the April 2017 Warrant is substantial evidence that they were acting in good faith. This conclusion is reinforced by the fact that, as Schulte concedes, all of the

information in the April and May Affidavits was true. This included not only that the CP Image was found on Schulte's Desktop Computer, but a detailed description of the CP Image and how it was potentially downloaded to the Desktop Computer. In addition, the affidavits were not a one-sided presentation of the information on which probable cause was based. Rather, the agents forthrightly disclosed the possibility that the CP Image might not actually have been child pornography at all and that it potentially was automatically downloaded from the Internet. These circumstances are markedly different than those in other cases in which courts have inferred recklessness based on an omission. *See, e.g.*, *Brown v. D'Amico*, 35 F.3d 97, 99 (2d Cir. 1994) (a "clear example" of an omission "critical" to the evaluation of probable cause "would occur if an officer secured a warrant by informing a judge that he heard the defendant utter a threat, but failed to mention that the officer knew that the defendant was reading lines while auditioning for a part in a play."); *Walczyk v. Rio*, 496 F.3d 139,161-62 (2d Cir. 2007) (probable cause existed only because the target allegedly maintained a second residence at the premises to be searched, but affidavit omitted the fact that the target had not resided there for more than seven years); *United States v. Liston*, 120 F.3d 965, 969 (9th Cir. 1997) (probable cause depended "entirely" on the connection between the target and the residence searched, but affidavit failed to disclose a large "for sale" sign posted on the lawn with a "sold" sign affixed to it for at least 30 days).

Indeed, if the agents in this case intended to deliberately or recklessly omit material information, they could have simply ignored the CP Image, not sought the Supplemental Warrants, and continued searching the Electronic Devices. Had the agents done so, however, the Government might now be facing a motion to suppress based on the FBI's failure to seek an additional warrant upon discovery of the child pornography and copyright offenses. *See, e.g.*, *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999) (suppressing child pornography

images found pursuant to the search of a computer for evidence of drug crimes because after the agent found the first image of child pornography he continued searching and seized other images of child pornography, thereby exceeding the scope of the warrant); *see also United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010) (noting that after an agent discovered "obvious evidence of child pornography" pursuant to a search for other materials, the agent's "failure to stop his search and request a separate warrant for child pornography [was] troubling"). The April and May Affidavits reflect that the agents adopted the opposite approach, and were cautious and diligent during a highly sensitive and urgent national security investigation, not deceptive or reckless. *See, e.g.*, *United States v. Lucas*, 640 F.3d 168, 180 (6th Cir. 2011) (upholding denial of motion to suppress where officer obtained consent to search the defendant's computer for evidence of drug trafficking and, upon discovering evidence of child pornography, immediately stopped searching until he obtained a search warrant for child pornography); *United States v. Koch*, 625 F.3d 470, 476 (8th Cir. 2010) (upholding search where officers immediately stopped their warrant-authorized search of the defendant's flash drive for evidence of gambling when they discovered child pornography).

B. Suppression Is Unwarranted Because the Government Would Have Inevitably Discovered the Child Pornography

Even if the Government arguably was not authorized to search for child pornography pursuant to the Supplemental Warrants, the Government inevitably would have discovered the child pornography during the search of the Electronic Devices authorized both by the Covert and Overt Warrants and the unchallenged portion of the Supplemental Warrants relating to the copyright offenses. As a result, Schulte's motion fails.

1. Relevant Facts

During the search of the Electronic Devices, FBI computer scientists (the "Computer Scientists") discovered a massive amount of apparent child pornography, principally in two

locations on the Desktop Computer. The Computer Scientists discovered this child pornography in plain view after unlocking hidden and/or encrypted compartments on the Desktop Computer.

By way of background, the Desktop Computer contained four storage devices, three of which were configured as an encrypted Raid 5 volume, that is, a data storage system that combines multiple drives into one unit (the "Raid 5 Volume"). (Declaration of FBI Computer Scientist Luis Cruz ¶ 3). As part of the Computer Scientists' review of the Desktop Computer, they decrypted the Raid 5 Volume and assessed its contents. (*Id.*).

Within the Raid 5 Volume, the Computer Scientists encountered an approximately 100 gigabyte partition containing an encrypted Linux Mint Virtual Machine (the "VM"). (*Id.* ¶ 4). "[A] virtual machine is a full computer system within a physical computer." (*Id.*). The Computer Scientists were able to access the VM by inputting a password obtained from the Electronic Devices, which Schulte used for other of his accounts. (*Id.* ¶ 4). Upon accessing the VM, the Computer Scientists discovered a user account "josh" with an encrypted home directory (the "Home Directory"). (*Id.* ¶ 5). The Computer Scientists were able to access the Home Directory by inputting a different password obtained from the Electronic Devices. (*Id.*).

Upon accessing the Home Directory, the Computer Scientists identified a file titled "data.bkp" that was approximately 50 gigabytes in size (the "Data File"). (*Id.* ¶ 6). Initially, when the Computer Scientists opened the Data File, the file appeared to contain only random data. Based on the size of the Data File and its contents, which appeared to be highly random data, and based on the presence of the encryption software VeraCrypt on the VM, the Computer Scientists determined that the Data File was potentially a VeraCrypt encrypted container. (*Id.* ¶ 7). The Computer Scientists were subsequently able to decrypt the Data File using VeraCrypt by entering the same password used to access the VM. (*Id.*).

Once the Data File was decrypted, it was immediately apparent from the names of the files that it likely contained a huge amount of child pornography. (*Id.*). For example, some of the file names included "(PHTC) Kelly 8Y0 – Sucking & Trying Fuck.avi"; "(pthc) TF-BTF-01 – Man Gets In Bed With Hot 7yo.mpg"; and "3+4yr 2 Girls children sexually abused BEAUTIFUL_Venezuela part-2. Mpg." (*Id.*). As a result, the Computer Scientists promptly contacted Agent Evanchec. After consulting with Agent Evanchec, the Computer Scientists opened several of the files, which appeared to contain child pornography. (*Id.* ¶ 8).

In addition, within the Data File, there was an additional file also titled "data.bkp" that was several gigabytes in size and that also contained random, binary data (the "Second Data File"). (*Id.* ¶ 9). The Computer Scientists were subsequently able to decrypt the Second Data File using VeraCrypt by entering the same password used to access the VM and the Data File, as described above. (*Id.*). Once the Second Data File was decrypted, it contained forensic artifacts of files having names indicative of child pornography. (*Id.*).

Finally, after identifying the Data File and Second Data File, the Computer Scientists also identified another VeraCrypt encrypted container within the Raid 5 Volume titled "volume," which appeared to contain over approximately 100 gigabytes of data (the "Volume Encrypted Container"). (*Id.* ¶ 10). The Computer Scientists were able to decrypt at least a portion of the Volume Encrypted Container. Once the Volume Encrypted Container was decrypted, it contained, among other things, additional images and videos (the "Additional Child Pornography"). The Additional Child Pornography was reviewed by members of the Crimes Against Children Squad who determined that it was, in fact, child pornography. (*Id.*).

Notably, in reviewing the foregoing locations on the Desktop Computer, the Computer Scientists did not use any forensic techniques, such as keyword searches, directed to identifying child pornography. (*Id.* ¶ 11).

2. Applicable Law

The exclusion of evidence is improper when the inevitable discovery doctrine applies. Under this doctrine, evidence that was illegally obtained will not be suppressed if the Government can "establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means." *Nix v. Williams*, 467 U.S. 431, 444 (1984). In meeting this burden, the Government must prove "that each event leading to the discovery of the evidence would have occurred with a sufficiently high degree of confidence for the district judge to conclude, by a preponderance of the evidence, that the evidence would inevitably have been discovered." *United States v. Vilar*, 729 F.3d 62, 84 (2d Cir. 2013). The ultimate question for any court weighing application of this doctrine is this: "Would the disputed evidence inevitably have been found through legal means but for the constitutional violation? If the answer is yes, the evidence seized will not be excluded." *United States v. Heath*, 455 F.3d 52, 55 (2d Cir. 2006).

The inevitable discovery doctrine is "an extrapolation from the independent source doctrine," which provides that evidence should not be suppressed where police obtain a valid warrant based on information which "came from sources wholly unconnected with the [illegal search] and was known to the agents well before the [illegal search occurred]. *Segura v. United States*, 468 U.S. 796, 814 (1984). The animating force behind these doctrines is a simple principle:

> [T]he interest of society in deterring unlawful police conduct and the public interest in having juries receive all probative evidence of a crime are properly balanced by putting the police in the same, not a worse, position than they would have been in if no police error or misconduct had occurred. When the challenged evidence has an independent source, exclusion of such evidence would put the police in a worse position than they would have been in absent any error or violation.

Nix, 467 U.S. at 443 (internal citation omitted).

3. Discussion

This is the quintessential case for application of the inevitable discovery doctrine. The simple question presented is whether law enforcement would have discovered the child pornography through lawful means had they never sought or obtained authorization to search the Electronic Devices for child pornography. *Heath*, 455 F.3d at 55. The clear answer to that question is yes—law enforcement would have continued searching the Electronic Devices for evidence of the Espionage Offenses pursuant to the Covert and Overt Warrants, and for evidence of the copyright infringement offenses pursuant to the unchallenged portion of the Supplemental Warrants. Pursuant to those lawful searches, the FBI inevitably would have discovered the child pornography in plain view on the Desktop Computer. In fact, that is precisely what happened.

As set forth above, the Computer Scientists worked methodically to unlock hidden and/or encrypted areas of the Desktop Computer and review or survey the files within those areas. The Covert and Overt Warrants explicitly authorized law enforcement to do so, providing that law enforcement could use various techniques to review electronically stored information for evidence of the Espionage Offenses including, among others: (i) "surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files)"; (ii) "conducting a file-by-file review by 'opening' or reading the first few 'pages' of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance)"; and (iii) "'scanning storage areas to discover and possibly recover recently deleted data or deliberately hidden files." (Ex. A ¶ 34).

During that search, the Computer Scientists encountered the Data File and the Volume Encrypted Container, both large files that appeared to be (and in fact were) VeraCrypt encrypted containers. Using Schulte's own passwords, the Computer Scientists decrypted those locations of the Desktop Computer and, upon decryption, it was apparent that they contained child pornography. Again, the Computer Scientists did not conduct any keyword searches for child pornography to identify those containers or to unlock them. (Cruz Aff. ¶ 11). Rather, it was entirely reasonable and appropriate for the Computer Scientists to focus on unlocking hidden and encrypted locations on the Desktop Computer in an effort to locate evidence of the Espionage Offenses and/or the copyright infringement offenses. (*Id.*).

On encountering images of child pornography while engaged in that lawful process, the Computer Scientists, even in the absence of the Supplemental Warrants, were entitled to seize the pornographic images and videos under the plain view exception to the warrant requirement. *Galpin*, 720 F.3d at 451 ("The plain view doctrine permits an officer to seize evidence outside a warrant's authorization when it is immediately apparent that the object is connected with criminal activity, and where such search and seizure do not involve an invasion of privacy." (internal quotation marks omitted)); *see also Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971) ("What the 'plain view' cases have in common is that the police officer in each of them had a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence incriminating the accused.").[11] Indeed, the plain view exception clearly would have

[11] Notably, the Fourth Amendment does not prohibit the warrantless seizure of evidence in plain view even though the discovery of the evidence was not inadvertent. *Horton v. California*, 496 U.S. 128, 136-41 (1990). Nevertheless, inadvertence is a characteristic of most plain-view seizures. *Id.* Here, as noted above, the child pornography would have been inadvertently discovered whether or not the FBI was authorized to seize evidence of child pornography.

applied here because the Computer Scientists had lawful access to the Electronic Devices, were authorized to identify and unlock hidden compartments on those devices and survey files within them, and, in that process, inadvertently encountered incriminating child pornography. *Horton*, 496 U.S. at 136; *Coolidge*, 403 U.S. at 465; *United States v. Crespo-Rios*, 645 F.3d 37, 43 (1st Cir. 2011) (denying motion to suppress child pornography seized pursuant to a computer search for other crimes where the Government would have inevitably discovered the child pornography by reviewing files on the computer); *United States v. Williams*, 592 F.3d 511, 521 (4th Cir. 2010) (upholding the admissibility of images of child pornography discovered while executing warrant for state law crimes of computer harassment); *see also United States v. Bonczek*, No. 08 Cr. 361 (PAC), 2008 WL 4615853, at *8-9 (S.D.N.Y. Oct. 16, 2008) (inevitable discovery doctrine applies where agents would have obtained a warrant even had they not unlawfully entered the defendant's apartment and discovered child pornography).[12]

Once the initial CP Image was discovered, as the April and May Affidavits make clear, the FBI promptly consulted with prosecutors and sought the Supplemental Warrants, which specifically authorized them to seize the CP Image and any other child pornography on the Electronic Devices. That is exactly what they should have done. *See Mann*, 592 F.3d at 786;

[12] Although the file labels for much of the child pornography identified on the Desktop Computer clearly indicated that the files likely contained child pornography, it was permissible for the Computer Scientists to review the files regardless of their file labels or extensions. *See, e.g., United States v. Highbarger*, 380 F. App'x 127, 130 (3d Cir. 2010) ("Suspects can easily hide information by mislabeling files, and, therefore, law enforcement officials are not required to accept a suspect's designation of what is contained in a particular file."); *Williams*, 592 F.3d at 522 ("Surely, the owner of a computer, who is engaged in criminal conduct on that computer, will not label his files to indicate their criminality."); *United States v. Harding*, 273 F. Supp. 2d 411, 424 (S.D.N.Y. 2003) ("Files containing graphical images may be assigned file extensions . . . that typically are assigned to text files. Files containing text may be assigned file extensions, including 'JPG' or 'GIF', that typically are given to graphical image files.").

United States v. Burgess, 576 F.3d 1078, 1092 (10th Cir. 2009) (distinguishing *Carey*, 172 F.3d 1268). Moreover, given the agents' actions, had they sought but not obtained authorization to search for child pornography based on the CP Image, the Court can have a "high level of confidence" that the agents would have sought an additional warrant at the time they identified the thousands of images of child pornography in the Data File and Volume Encrypted Container. *Heath*, 455 F.3d at 55; *see also Bonczek*, 2008 WL 461583, at *8 ("Additionally, the Court has a 'high level of confidence,' as required by *Heath*, 455 F.3d at 55, that police would have obtained a warrant based on what they knew prior to the illegal entry, and that they would have discovered the same evidence even if they had waited for the warrant before entering."). There can be no reasonable dispute that an affidavit submitted in support of such a warrant would have presented overwhelming evidence justifying the seizure of child pornography on the Electronic Devices.

Based on the foregoing circumstances, it is clear that the child pornography on the Desktop Computer would have been inevitably discovered and that suppression is entirely unwarranted.

III. THE 2017 WARRANTS ARE APPROPRIATELY PARTICULARIZED

In line with the Fourth Amendment's requirements, the 2017 Warrants identified the crimes under investigation and set forth specific categories of evidence subject to seizure such that any executing officer could easily "ascertain and identify with reasonable certainty those items that the magistrate judge authorized him to seize." *George*, 975 F.2d at 75. Schulte misconstrues the Warrants' provisions and the contours of controlling precedent. The 2017 Warrants were particularized and each category of evidence subject to seizure was supported by probable cause.

First, Schulte acknowledges that much "of the sought information came with qualifying language" related to the Subject Offenses, but argues that these qualifiers did "no work" because agents "could not know whether or not [Schulte's electronic information] 'related to the Subject

Offenses' without reading it." (*See* Res. Br. 43). But the Second Circuit has realized that, in searches for documents and records, "some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990) (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)). There is nothing overbroad about a search warrant that simply permits agents to search records to see if they fit within the warrant's parameters.

Second, Schulte argues that the portions of the 2017 Warrants that authorize the search and seizure of evidence (i) required to access seized electronic media (*e.g.*, login credentials or passwords), (ii) that could facilitate a forensic examination of seized electronic (*e.g.*, user manuals), and (iii) about the access to, ownership, or control over seized media, were not limited by reference to the Subject Offenses and thus were overbroad. (*See* Res. Br. 44). But Schulte's argument makes no sense. Subparagraphs 4 and 5 of Section III.A of the Covert Warrant, for example, states that the FBI could seize electronic devices, storage media, and electronic forensic evidence that was "used in furtherance of the Subject Offenses, containing evidence of the Subject Offenses," or "relating to the Subject Offenses," or which pertained to the "occupancy and ownership of" Schulte's home, the identity and location of any co-conspirators, or the unauthorized retention, gathering, or transmission of classified information. Evidence described in the categories in Section III.B would simply allow the FBI to access or determine the user of electronic media that was seized because it had a connection to the Subject Offenses. That type of evidence cannot logically be limited by reference to the Subject Offenses—it makes no sense, for example, to say that a user manual or password relates to a Subject Offense. And similarly, evidence of ownership cannot be cabined to the Subject Offenses—records showing that Schulte, for example,

owned the Desktop Computer on which the child pornography was found is evidence, even if it, does not, on its face, tie to a Subject Offense. These categories of evidence are particularized.[13]

Finally, Schulte argues that the 2017 Warrants lack particularity because they are not confined to a date range. (Res. Br. 44-45). There is no law in this Circuit requiring a warrant to include a temporal limitation. The cases Schulte cites in this regard relate to searches of business records, not computer data, and in any event stand, at best, for the proposition that the Government should include a temporal limitation "when possible." *United States v. Levy*, 2013 WL 664712, at *11 n.7 (S.D.N.Y. 2013). In *United States v. Wey*, 256 F. Supp. 3d 355, 387 (S.D.N.Y. 2017), for example, the court criticized the Government for not including a temporal limitation in the warrant when the Government otherwise had identified relevant timeframes and dates of interest in the supporting affidavit and indictment. Thus, the *Wey* court was concerned that the Government had knowledge of appropriate temporal limitations, but did not include those limitations in the warrant. Nonetheless, *Wey* was clear that a temporal limitation is not a "universal requirement" and instead is a "circumstance-specific" consideration in evaluating the particularity of a warrant. *Id.* at 381.

Here, unlike in *Wey*, at the time the Government submitted the Covert Warrant, mere days after the March 7 Leak, the Government had not identified any facts suggesting that a limited timeframe was appropriate and, indeed, the nature of the offense counseled otherwise. Although Schulte argues that March 2016 would have been appropriate, there is no reason to believe that relevant evidence would not have existed from long before that. For example, the FBI did not

---

[13] Even if the contested categories were not sufficiently particularized, the remedy is not suppression of all seized data, as Schulte requests, but rather severance of data collected pursuant to the deficient categories. Indeed, "[w]hen a warrant is severable, the portion of the warrant that is constitutionally infirm—usually for lack of particularity or probable cause—is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid portion may be admitted." *Galpin*, 720 F.3d at 448) (internal quotation marks omitted).

know when, if at all, Schulte had first been in contact with or had developed an interest in WikiLeaks, which was established in 2006, or whether Schulte had transmitted the information through other intermediaries that he had known before. Moreover, as the Covert Affidavit made clear, WikiLeaks stated that it had additional classified information that it intended to disclose, and the FBI did not know if all of that information was disclosed as part of one incident or if the illegal disclosures had occurred over years (particularly since Schulte had worked at the CIA since 2011). The same is true with respect to Schulte's disgruntlement—although Schulte's attitude appeared to have changed in February 2016, the FBI did not know for how long Schulte's anger had been simmering. Common sense dictates that trying to determine when and how a person developed the willingness to betray the oath he took at the CIA and publicly disclose some of the United States' most closely guarded secrets requires examining records over a long time period.

Moreover, in considering the scope of the information sought, it is relevant that the Covert Warrant was drafted just days after the initial Leak—one of the largest, if not the largest, disclosure of CIA classified information—at a time when it seemed that other disclosures were imminent. *Bianco*, 998 F.2d at 1115 (collecting cases in which "the government was under emergency pressures that necessitated a broadly worded warrant"), *abrogated on other grounds by Groh v. Ramirez*, 540 U.S. 551 (2004); *Young*, 745 F.2d at 759 (noting that courts tolerate a greater degree of ambiguity where agents have done the best they reasonably could under the circumstances). While the Government is not suggesting that a temporal limitation on a warrant would never be appropriate in a national security case, the "circumstance-specific considerations" here weigh against inclusion of a temporal limitation. *Wey*, 256 F. Supp. 3d at 381. Ultimately, the Government "describe[d] the items to be seized with as much particularity as the circumstances reasonably allow[ed]," *Galpin*, 720 F.3d at 446, which is what the law requires.

IV. THE EVIDENCE SEIZED PURSUANT TO THE MCC WARRANTS SHOULD NOT BE SUPPRESSED

Schulte also moves to suppress certain evidence recovered from the MCC. But his argument that suppression is appropriate because the FBI purportedly violated his attorney-client privilege misses the mark—as with all of the other warrants in this case, the FBI acted cautiously by, among other things, seeking authorization from the Court to use a wall team to screen out any privileged materials. Schulte's motion fails as a matter of law, and no hearing is required.

A. Relevant Facts

On October 2, 2018, the Government applied for the MCC Premises Warrant, which sought authorization to search two units at the MCC (including the one in which Schulte was housed) and the MCC's law library (the "MCC Premises"). (Ex. F ¶ 3). In the affidavit, the affiant, Agent Donaldson, first described the circumstances of Schulte's detention at the MCC (including his theft of the Classified Information) (*id.* ¶¶ 8(a)-(f)), and that Schulte was housed in the same unit as another inmate, Omar Amanat, who had been convicted of fraud offenses and who had fabricated evidence at trial (*id.* ¶¶ 9 & 12). Agent Donaldson went on to state that, in or about April 2018, Schulte sent at least one of the 2017 Warrants to a reporter in violation of the Court's protective order, resulting in the Court's reprimand on May 21, 2018. (*Id.* ¶¶ 11(a)-(d)). Finally, Agent Donaldson described information that the FBI had received from another inmate (the "CS"), who had informed the FBI that, among other things, Schulte and Amanat were using Contraband Cellphones in the MCC, and that the CS recalled at least one conversation over one of the Contraband Cellphones in which "Vault 7," the name for the 2017 WikiLeaks disclosures, had been discussed. (*Id.* ¶ 13). The CS also provided the FBI with screenshots and videos of Schulte and Amanat using the Contraband Cellphones to, among other things, disseminate documents they had drafted. (*Id.* ¶ 15). Based on this application, the Court authorized the search of the MCC

Premises, including for the Contraband Cellphones and any documents and records pertaining to the illegal gathering, retention, removal, and transmission of classified information, including in particular nine "articles" Schulte had drafted (the "Schulte Articles"). (*Id.* ¶ 6).

On October 3, 2018, the FBI began to search the MCC Premises. During the search, MCC officials gave the FBI documents from the cell Schulte inhabited before his transfer to a secure housing unit on October 1, 2018 (the "Schulte Cell Documents"), including loose files, as well as several notebooks and notepads (the "Notebooks," one of which is attached as Classified Exhibit M). The cover of each of the Notebooks was labeled with the words "ATTORNEY-CLIENT PRIVILEGE."[14] Agent Donaldson and FBI Special Agent Evan Schlesinger flipped briefly through the Schulte Cell Documents and confirmed that they appeared to contain handwritten text potentially written by Schulte. The agents opened to a small subset of pages in each Notebook at random, and made a cursory examination of the legible text on those pages. During that review, the agents identified some writings that appeared to be potentially classified. The agents, however, were not sure whether these documents fell within the ambit of the MCC Premises Warrant. Among some of the loose files, the agents also saw, among other things, cover pages marked with Trulincs, which the agents understood might relate to Schulte's defense.

Based on these findings, the agents immediately informed the prosecutors about the discovery of the Schulte Cell Documents. The prosecutors told the agents to stop reviewing the Schulte Cell Documents until the prosecutors had given the FBI further instruction. The

[14] Because the MCC searches were valid even if Schulte's factual assertions were true, the Government does not believe that a hearing is necessary. If the Court were, however, to hold a hearing on the MCC searches, the Government anticipates that the agents would testify that they do not recall seeing these notations on the covers of the Notebooks before they began to review them. As noted above, however, the agents did see certain documents in the Schulte Cell Documents that they believed might be potentially privileged (and therefore did not review), which is one of the reasons they contacted the prosecutors.

Government then sought the MCC Wall Warrant for authorization to search the Schulte Cell Documents for evidence of the same crimes as those identified in the MCC Premises Warrant. Because the agents had noticed potentially privileged documents, the Government sought authorization to implement a wall review process for searching the Schulte Cell Documents.

In the affidavit for the MCC Wall Warrant, Agent Donaldson stated that "before the search began, MCC officials had removed the Schulte Cell Documents, among other things, from Schulte's former cell and stored them in an official office at the MCC." (Ex. G ¶ 6(a)). The Schulte Cell Documents were "comprised of approximately 300 pages of material," which the FBI agents "began to review" during the search of the MCC Premises. (*Id.* ¶ 6(b)). During that initial review, Agent Donaldson described how the agents had found, among other things, copies of the Schulte Articles, an email account that was accessed from one of the Contraband Cellphones and the password to that account (the "John Smith Document"), and a document purportedly authored by an FBI agent (the "FBI Document") and intended for WikiLeaks, in which the author claimed that Schulte was not responsible for the Leaks and that the FBI had planted child pornography on Schulte's computer. (*Id.*). The agents also saw, however, some markings on the documents that indicated that some of the documents "were potentially prepared to aid in Schulte's defense." (*Id.* ¶ 6(c)). As a result, the Government sought to implement a wall review team (the "Wall Team"), that would review the Schulte Cell Documents for any privileged material and then turn over any non-privileged material to the FBI case agents to review. (*Id.* ¶ 7). That review was to be completed within 48 hours. (*Id.* ¶ 8). The Court granted the Government's application.

Within the prescribed time, the Wall Team reviewed the Schulte Cell Documents, redacted material that the Wall Team had determined to be privileged, and provided the redacted versions to the case team. The Wall Team also provided both redacted and unredacted copies of the Schulte

Cell Documents to the defense. The Government also provided the redacted versions of the Schulte Cell Documents to the CIA for a classification review. In reviewing the redacted versions of the Schulte Cell Documents, the case team noted that, in addition to the John Smith Document and the FBI Document, the Schulte Cell Documents also included among other things, (i) information about social media (the "Social Media Accounts") and encrypted email accounts (the "Encrypted Accounts") that Schulte had or intended to create, including passwords for those accounts (*see, e.g.*, Ex. M at 113); (ii) a draft tweet that contained classified information and in which Schulte purported to be one of his former CIA colleagues, who claimed that the CIA had framed Schulte (the "Fake Tweet") (*id.* at 131-32); (iii) threats by Schulte to begin an "information war" against the United States, during which he would disclose additional classified information, unless he was released and paid restitution (*id.* at 97), (iv) Schulte's list of steps to destroy evidence, including deleting "suspicious emails" from accounts he was using in prison (*id.* at 112-13); (v) Schulte's notations to "DL Disc. UL WL," which the FBI understood to likely mean downloading Schulte's discovery ("DL Disc.") and uploading it to WikiLeaks ("UL WL") and to "schedule tweets" (*id.* at 148); (vi) notes about apparent segments of memory in a laptop where data could be hidden—a laptop that the Government had given Schulte to review discovery (*id.* at 101); (vii) a note to "check Galaxy [*i.e.* the model of one of the Contraband Cellphones] for Signal," an encrypted messaging application (*id.* at 140); and (ix) a loose "article" titled "Malware of the Mind" (the "Malware Article," attached as Exhibit N) addressed to the technology community, which contained classified information about Schulte's CIA training.

Based in part on these findings, the Government applied for additional search warrants including the Encrypted Email Warrant; the Social Media Warrant; and the Laptop Warrant. The Court granted the Government's application for each of these Warrants. The searches conducted

pursuant to these Warrants also uncovered significant evidence against Schulte, including an email that he sent to a reporter in September 2018, in which Schulte claimed to be a third party speaking on Schulte's behalf and attached a document that purportedly rebutted the probable cause in one of the 2017 Warrants and contained classified information.

B. Applicable Law

1. Execution of a Search Warrant

The Fourth Amendment does not require an authorizing court to approve the manner in which a search will be conducted. Rather, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant." *Dalia v. United States*, 441 U.S. 238, 257 (1979). Ultimately, "the Government's review need only be reasonable, not perfect, and law enforcement is given significant latitude in determining how to execute a warrant." *United States v. Lumiere*, No. 16 Cr. 483 (JSR), 2016 WL 7188149, at *6 n.9 (S.D.N.Y. Nov. 29, 2016).

Inherent in the execution of a search is the review of items that may not ultimately fall within the scope of the seizure. *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) ("[I]t is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."). "[T]he Fourth Amendment is not violated because the officers executing the warrant must exercise some minimal judgment as to whether a particular document falls within the described category [subject to seizure]." *United States v. Riley*, 906 F.2d 841, 843-45 (2d Cir. 1990). Rather, "allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked '[crime] records.'" *Id.* at 845; *see also United States v. Alexander*, 1993 WL 97407, at *7 (S.D.N.Y. 1993) (citing *Riley* for the proposition that "a warrant

authorizing seizure of records of criminal activity allows officers some latitude to examine many papers"); *United States v. Milan-Colon*, 1992 WL 236218, at *28 (S.D.N.Y. 1992) (same); *see also United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 62-63 (D. Conn. 2002).

2. Attorney-Client Privilege and Search Warrants

The burden to establish that information is privileged unequivocally rests with the defendant. *See United States v. Schwimmer*, 892 F.2d 237, 244 (2d Cir. 1989). "To invoke the attorney-client privilege, a party must demonstrate that there was: (1) a communication between client and counsel, which (2) was intended to be and was in fact kept confidential, and (3) made for the purpose of obtaining or providing legal advice." *United States v. Constr. Prods. Research, Inc.*, 73 F.3d 464, 473 (2d Cir. 1996). Thus, the privilege does not attach to communications between two or more persons that do not enjoy an attorney-client relationship. *Schwimmer*, 892 F.2d at 243 ("The relationship of attorney and client, a communication by the client relating to the subject matter upon which professional advice is sought, and the confidentiality of the expression for which the protection is claimed, all must be established in order for the privilege to attach."). Additionally, it is settled that even where an attorney-client relationship does exist, disclosure of a privileged communication to a third party waives privilege as to that communication. *See Schaeffler v. United States*, 806 F.3d 34, 40 (2d Cir. 2015) (privilege "is generally waived by voluntary disclosure of the [privileged] communication to another party").

To protect against the disclosure of attorney-client material during the execution of a search warrant, courts in this district have approved of a "common procedure" of designating a filter or wall team. *United States v. Ceglia*, 2015 WL 1499194, at *1 (S.D.N.Y. 2015); *United States v. Feng Ling Liu*, 2014 WL 101672, at *11 (S.D.N.Y. 2014): *see also Lumiere*, 2016 WL 7188149, at *7 n.10 (noting that the Government proposed using a "'wall' protocol if it becomes aware of

privileged documents, . . . which may well moot [the defendant's suppression motion] entirely.").[15] The Government's use of a wall team is evidence of the Government's good faith. *See United States v. Patel*, 2017 WL 3394607, at *7 (S.D.N.Y. 2017) (the Government's use of a wall review team after identifying potentially privileged documents "do[es] not evidence the sort of bad faith or flagrant disregard of the warrant's limits that would justify the wholesale suppression of evidence"); *SEC v. Lek Secs. Corp.*, 2018 WL 417596, at *4 (S.D.N.Y. 2018) (stating that the SEC's use of a filter team "reflects respect for the privilege").

Courts approve wall teams—even over *a priori* objections—because, among other reasons, vital Government and public interests may otherwise be impinged. *See, e.g., United States v. Winters*, 2006 WL 2789864, at *6 (S.D.N.Y. 2006) (adopting the Government's proposed use of a "'wall Assistant'" because the defendant's proposal of *in camera, ex parte* review "though perhaps more protective of the privilege, does not adequately account for society's interest in the enforcement of its criminal law"); *United States v. Grant*, 2004 WL 1171258, at *2 (S.D.N.Y. 2017) ("Although some of these documents likely contain attorney-client privileged communications, the Government should be allowed to make fully informed arguments as to privilege if the public's strong interest in the investigation and prosecution of criminal conduct is to be adequately protected."); *Stewart*, 2002 WL 1300059, at *5 ("[T]he [attorney-client] privilege

[15] Although certain decisions in this district have expressed some disapproval of the Government's use of wall teams to screen for privileged material, *see United States v. Kaplan*, 2003 WL 22880914, at *4 n.4, *12 (S.D.N.Y. 2003); *United States v. Stewart*, 2002 WL 1300059, at *6 (S.D.N.Y. 2002); *In re Search Warrant for Law Offices Executed on March 19, 1992*, 153 F.R.D. 55, 59 (S.D.N.Y.1994), none of those cases suggests that this practice necessitates the suppression of evidence, *see Kaplan*, 2003 WL 22880914, at *11 ("[N]either *Stewart* nor *In re Search Warrant* require this Court to employ methods beyond those already used to safeguard potentially privileged materials from disclosure and review."); *see also Hempstead Video, Inc. v. Inc. Vil. of Valley Stream*, 409 F.3d 127, 137 (2d Cir. 2005) ("[A] few district courts have drawn a tentative inference that our Circuit may categorically reject the efficacy of isolation efforts as protection against taint. . . . This would be a mistaken reading of our precedents.").

is itself based in policy, rather than in the Constitution, and therefore it alone 'cannot stand in the face of countervailing law or strong public policy and should be strictly confined within the narrowest possible limits underlying its purpose.'" (quoting *United States v. Goldberger & Dubin, P.C.*, 935 F.2d 501, 504 (2d Cir. 1991)); *see also United States v. Int'l Bhd. of Teamsters*, 119 F.3d 210, 214 (2d Cir.1997) ("[S]ince the attorney-client privilege stands in derogation of the public's right to every man's evidence, it ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle." (ellipsis omitted)).

Finally, even if law enforcement seizes privileged material alongside information responsive to the warrant, it is well settled that the proper remedy is suppression of the privileged material—not wholesale suppression of the entire search. *See, e.g.*, *Nat'l City Trading Corp. v. United States*, 635 F.2d 1020, 1026 (2d Cir. 1980) (in the context of a search of a law office pursuant to a search warrant, "[t]o the extent that the files obtained here were privileged, the remedy is suppression and return of the documents in question, not invalidation of the search" (citation omitted)); *Patel*, 2017 WL 3394607, at *6 ("'The general remedy for violation of the attorney-client privilege is to suppress introduction of the privileged information at trial,' not to order wholesale suppression." (quoting *Lumiere*, 2016 WL 7188149, at *6)); *Feng Ling Liu*, 2014 WL 101672, at *11 (same); *United States v. Chuang*, 696 F. Supp. 910, 915 (S.D.N.Y. 1988) (same); *United States v. Giovanelli*, 747 F. Supp. 891, 894 (S.D.N.Y. 1989) (refusing to suppress the entirety of a notebook seized by the Government where at least portions of the notebook were properly seized). "[T]he drastic remedy of the suppression of all evidence seized is not justified unless those executing the warrant acted in flagrant disregard of the warrant's terms." *United States v. Matias*, 836 F.2d 744, 747-48 (2d Cir. 1988) (citing cases); *see also Kaplan*, 2003 WL 22880914, at *11 (suppressing evidence where law enforcement disregarded court-ordered

procedures, including by allowing the case agent, rather than the wall-team prosecutors, to determine if crime-fraud exception applied).

C. Discussion

1. The Notebooks Were Subject to Seizure

Schulte's initial claim that the MCC Premises Warrant did not authorize seizure of the Schulte Cell Documents, and in particular, the Notebooks, is entirely without merit. As described above, the MCC Premises Warrant authorized the FBI to search for and seize, among other things, evidence of the smuggling and use of the Contraband Cellphones and documents pertaining to the unlawful retention, gathering, and transmission of classified information. *See supra* pp. 59-63. The Notebooks contained such evidence, including the John Smith Document—which described a covert email account Schulte was using—and the FBI Document—which is a false exculpatory statement related to Schulte's prior illegal transmission of classified information. *Id.*

Moreover, to the extent there was any ambiguity in the reach of the MCC Premises Warrant, the MCC Wall Warrant explicitly authorized the seizure of any documents, like the FBI Document, that reflected an attempt to obstruct justice or the smuggling in of the Contraband Cellphones or, as specified in the MCC Premises Warrant, evidence related to the unlawful handling of classified information. (Ex. G, Att. A III.A(b)-(c)). And the subsequent review of the Notebooks after the execution of the MCC Wall Warrant showed additional evidence subject to seizure, including documents containing classified information, like the Fake Tweet and the Malware Article; notes concerning the potential dissemination of Schulte's writings and discovery through social media; notes concerning the use of the Encrypted Email Accounts that were accessed from the Contraband Cellphones; and notes about an encrypted messaging application

that Schulte wanted to download to one of the Contraband Cellphones. All of these plainly fell within the ambit of the MCC Premises Warrant and the MCC Wall Warrant.

The fact that some of the pages in the Notebooks may have contained irrelevant or privileged information does not preclude the Notebooks' seizure, but instead means only that those irrelevant or privileged parts may not be used against the defendant. *See, e.g.*, *Giovanelli*, 747 F. Supp. at 894 ("[i]f the notebook does contain other statements alleged to be within the scope of Giovanelli's attorney-client privilege, and if the Government seeks to introduce those statements at trial, the court will determine at the proper time whether those statements may be correctly received in evidence"). Nevertheless, to the extent a Notebook contained relevant evidence, the entire Notebook was subject to seizure. The seizure of the entire document but use of only the relevant portions of the document is standard. For example, the fact that a narcotics trafficker's ledger may intermingle notations of innocent transactions with criminal ones does not mean that the seizing agents must excise out the criminal transactions at the scene of the search and leave behind the benign ones. Schulte's argument would require the Government to essentially tear out the relevant pages, thereby altering the original evidence. Indeed, following that approach would likely lead defendants like Schulte to claim that the FBI had tampered with the evidence.

2. The Government Did Not Act in Bad Faith by Confirming the Notebooks Were Subject to Seizure Before Seizing Them

Schulte's assertion that his labeling of the notebooks as "Attorney-Client Privileged" barred the executing agents from opening them and discovering that they were subject to seizure is equally meritless. Any search of documents for evidence necessarily involves some review of innocuous documents. *See Riley*, 906 F.2d at 845; *see also Andresen*, 427 U.S. at 482 n.11. Nor were the agents required to take Schulte's notation at face value, but could instead determine whether the Notebooks had any information relevant to the MCC Premises Warrant. *See, e.g.*,

Triumph Capital, 211 F.R.D. at 60–61 (executing agent "was not required to assume that document and file names and suffixes accurately described their contents, and he acted reasonably in manually reviewing documents and files to ascertain their relevance"). Given that the Notebooks did have relevant information, *see supra* pp. 59-63, the FBI agents cannot be faulted for briefly reviewing the Notebooks, contacting the prosecutors, and then seeking the MCC Wall Warrant.

Schulte's attempt to manufacture bad faith on the part of the FBI therefore fails completely. The fact that the FBI and the Government sought to implement a wall team demonstrates that the investigators were acting in good faith. *See Patel*, 2017 WL 3394607, at *7 (Government use of wall review team was evidence of good faith); *Lek*, 2018 WL 417596, at *4 (same). Moreover, contrary to Schulte's contention, the fact that the FBI and the Government sought the MCC Wall Warrant despite the urgency of the search further bolsters their good faith. While Schulte claims that there was no exigency, he ignores that, at the time of the MCC Premises search, the FBI knew only that a former, disgruntled CIA employee with knowledge of the CIA's tools, methods, sources, and operations, and charged with one of the largest leaks in the nation's history had secretly smuggled into the MCC illegal cellphones and was using them to communicate over encrypted email accounts about disseminating "articles" publicly, at least one of which contained classified information. It was imperative that the FBI determine what Schulte had disclosed, so that the Government could mitigate the damage. The fact that the Government nevertheless sought the MCC Wall Warrant "reflects respect for the privilege." *Lek*, 2018 WL 417596, at *4.

The urgency of the situation also defeats Schulte's criticism of the wall procedure ultimately implemented. Schulte claims that, like some other cases in this district, the appropriate procedure would have been for the Wall Team to first turn the materials over to the defense team, who could have objected and litigated the issue, before turning them over to the case team. The

wall procedure in this case was blessed by the Court, however, and for good reason. The situation presented by this case was unlike any of those Schulte cites. Here, the FBI was in the middle of an urgent investigation to determine what classified information Schulte had disseminated. Building in the back-and-forth between defense counsel and the Wall Team would inevitably have slowed the investigation dramatically. Adopting instead the time-worn practice of having the Wall Team screen the materials and turning them over to the case team properly balanced Schulte's interests with those of the public.

Schulte makes much of the fact that large portions of the Notebooks were redacted and that there were Post-It notes on certain relevant pages,[16] arguing that this shows that the case agents did a searching review of the Notebooks before obtaining the MCC Wall Warrant. His factual assertions are false, but even on its face Schulte's argument is inconsistent with the fact that the MCC Wall Warrant was sworn out on the same day as the search of the MCC Premises. If, as Schulte claims, the FBI had been willing to do a penetrating analysis of Schulte's privileged materials, then it makes no sense that the FBI agents alerted the Government to the potentially privileged material so quickly. Instead, the agents could simply have waited, reviewing the information at their leisure, and contacted the prosecutors days or weeks later, after the agents had time to dissect Schulte's privileged material. The fact that the agents contacted the prosecutors that very day shows that what really happened was that they did a cursory review of the Notebooks, skimming to see if material appeared responsive or privileged. That is entirely consistent with the

[16] The Government notes that, as the Wall attorney conveyed to defense counsel, the Wall Team flagged portions of the Notebooks that appeared to have privileged or responsive material with Post-Its. The agents who were involved in the initial review of the Notebooks at the MCC, on the other hand, did not use Post-Its. In addition, while Schulte makes much of the volume of redactions, out of an abundance of caution, the Wall attorney redacted material that, though not privileged, appeared to be non-responsive on its face.

agents' responsibility not only to be mindful of Schulte's privilege, but also their "duty to protect from disclosure sensitive information that could compromise national security." *United States v. Hashmi*, 621 F. Supp. 2d 76, 80 (S.D.N.Y. 2008).

3. Evidence From the MCC Warrants Should Not Be Suppressed Because the FBI Allegedly Seized Privileged Information

Schulte also claims that the Wall Team failed to redact a substantial amount of privileged information, but he musters few examples in his motion. Schulte's claim that the Notebooks continue to contain a significant amount of privileged information is highly dubious, given that, despite having received the Notebooks in discovery several months ago, Schulte has never contacted the Wall Team to ask that additional portions of the Notebooks be clawed back and redacted. That is even true for the Malware Article, which the Government specifically identified to the defense as being one of the bases for the most recent espionage charge on April 29, 2019. Schulte's decision to sit on his hands in the face of that disclosure and instead now seek suppression based on that same information suggests that his motion is simply gamesmanship.

Indeed, the Malware Article was, by its own terms, intended to encourage members of the technological community to come to Schulte's aid. The fact that this "article" was intended to be transmitted to third parties defeats any claim of privilege. *See Schaeffler*, 806 F.3d at 40; *In re Grand Jury Proceedings*, 2001 WL 1167497, at *7 (S.D.N.Y. 2001) ("Excluded from the attorney-client privilege are communications that were intended to be passed on to a third party."). That is true even if that information was shared with an attorney, as Schulte claims. *In re Grand Jury Proceedings*, 2001 WL 1167497, at *7 ("Indeed, although communications between a client and

an attorney may have been made privately, they are not privileged if the information was intended to be passed on to third parties.").

Moreover, even though Schulte points to some arguably privileged information that was improperly released (none of which the Government intends to introduce at trial), like Guidelines calculations or notes on search warrants (*see* MCC Br. 16), the remedy is suppression of those specific privileged items, not blanket suppression. *See Nat'l City Trading Corp.*, 635 F.2d at 1026; *Patel*, 2017 WL 3394607, at *6 ("The general remedy for violation of the attorney-client privilege is to suppress introduction of the privileged information at trial, not to order wholesale suppression."). Blanket suppression is particularly inappropriate given that the agents plainly acted in good faith by stopping their search upon discovering potentially privileged information and seeking the MCC Wall Warrant. *Matias*, 836 F.2d at 747 (blanket suppression "is not justified unless those executing the warrant acted in flagrant disregard of the warrant's terms.").

Schulte's argument for suppression of evidence seized pursuant to the subsequent Encrypted Account, Social Media, and Laptop Warrants is equally meritless. He claims that without the information in the Notebooks, the FBI would not have sought these Warrants. As described above, the FBI properly seized the Notebooks pursuant to the MCC Premises Warrant. *See supra* pp. 59-63. Thus, the only way suppression would be warranted is if the subsequent MCC Warrants relied on privileged information in the Notebooks, which Schulte cannot show. The fact that Schulte maintained encrypted email accounts with certain passwords to communicate with reporters and other outsiders, or noted locations on the Laptop where he could hide data, is unrelated to a request for legitimate legal advice. *See Constr. Prods. Research*, 73 F.3d at 473 (privileged communications must pertain to a request for legal advice). Similarly, the fact that

Schulte had declared an "information war" against the United States and intended to disclose additional classified information (*i.e.*, commit another crime) is not privileged.

Moreover, Schulte claims that the FBI read his thoughts on severance (which the Government has consented to) or a plea offer (which the Government has not made), but none of those "thoughts" are referenced in any subsequent search warrant. Indeed, Schulte's entire request for a hearing is premised on his speculation that there were investigative steps taken that extended beyond investigating the Contraband Cellphones, the Encrypted Accounts, the Social Media Accounts, or the Laptop. There were not. Schulte's motion for suppression should be denied.

V. THE GOOD FAITH EXCEPTION APPLIES

Even if a warrant is defective, the seized evidence may still be admitted under certain circumstances, including the good faith exception. The Supreme Court, in *United States v. Leon*, 468 U.S. 897 (1984), held that the exclusionary rule "does not apply to evidence seized 'in objectively reasonable reliance on' a warrant issued by a detached and neutral magistrate judge, even where the warrant is subsequently deemed invalid." *United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008) (quoting *Leon*, 468 U.S. at 922). The *Leon* Court explained that, "assuming that the [exclusionary] rule effectively deters some police misconduct and provides incentives for the law enforcement profession as a whole to conduct itself in accord with the Fourth Amendment, it cannot be expected, and should not be applied, to deter objectively reasonable law enforcement." *Leon*, 468 U.S. at 919. The Supreme Court has made clear that "the exclusionary rule is not an individual right and applies only where it results in appreciable deterrence." *Herring v. United States*, 555 U.S. 135, 141 (2009) (internal quotation marks and brackets omitted).

Under the good faith exception, evidence seized pursuant to an invalid search warrant will be suppressed only if (i) the issuing judge was knowingly misled; (ii) the issuing judge wholly

abandoned his or her judicial role; (iii) the application was so lacking in indicia of probable cause as to render reliance upon it unreasonable; or (iv) the warrant is so facially deficient that reliance upon it is unreasonable. *Falso*, 544 F.3d at 125. The central question is "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922 n.23. If the court finds that the officer's reliance on the warrant was objectively reasonable, suppression is not warranted. *Id.* at 922; *Davis v. United States*, 564 U.S. 229, 238 (2011). To trigger the exclusionary rule, law enforcement "conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 144.

In this case, even if the Court does determine that any of the Challenged Warrants are deficient, then the evidence seized pursuant to that warrant or warrants still should not be suppressed. A magistrate judge signed each of the Challenged Warrants, which is "the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in 'objective good faith.'" *Messerschmidt v. Millender*, 565 U.S. 535, 546 (2012) (quoting *Leon*, 468 U.S. at 922-23). Moreover, none of the exceptions that typically preclude application of the good faith doctrine applies here. As discussed above, with respect to each of the Challenged Warrants, there is no credible evidence that any of the affiants "knowingly misled" the magistrate judge. *See supra* pp. 31-33, 45-48. The Challenged Warrants also contain ample probable cause, even correcting any alleged misrepresentations or omissions, *see supra* pp. 20-31, 41-45, and it cannot be said that the magistrate judges who authorized these searches "wholly abandoned their judicial role." Finally, the Challenged Warrants carefully articulated tailored categories of evidence to be searched for and seized and thus cannot be facially invalid. *See Levy*, 2013 WL 664712, at *10 ("The Search Warrant here, however, cannot be said to be 'so facially deficient' as

to preclude reasonable reliance where it expressly provided that the officers were authorized to seize '[e]vidence, fruits, and instrumentalities of violations of [particular statutes].'").

Finally, with respect to Schulte's arguments about the lack of a temporal requirement, law enforcement agents certainly cannot be expected to adopt a particularity requirement that has not been imposed by the Second Circuit, even if some district courts have found such a consideration relevant to evaluating the parameters of a particular warrant. *See, e.g.*, *Levy*, 2013 WL 664712, at *10 ("The Court need not resolve whether the lack of a time limit renders the Search Warrant unconstitutional because the continuing uncertainty in this Circuit regarding this issue triggers the good-faith exception to the exclusionary rule."). Schulte's suppression motions thus should be denied even if the Court finds a deficiency in any of the Challenged Warrants.

CONCLUSION

Accordingly, the Government respectfully requests that the Court deny Schulte's suppression motions without a hearing.

Dated: New York, New York
August 2, 2019

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

by: /s/
Matthew Laroche
Sidhardha Kamaraju
Assistant United States Attorneys
Scott McCulloch
Trial Attorney, National Security Division

cc: Defense counsel of record (by hand and ECF)