UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA :

17 Cr. 548 (PAC)

-v- :

JOSHUA ADAM SCHULTE,

Defendant. :

----------X

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT JOSHUA ADAM SCHULTE'S MOTION TO SUPPRESS EVIDENCE OBTAINED IN VIOLATION OF THE FOURTH AMENDMENT

Federal Defenders of New York, Inc.
Counsel for Defendant **Joshua Adam Schulte**
52 Duane Street, 10th Floor
New York, New York 10007
Tel.: (212) 417-8713

Sabrina P. Shroff
Edward S. Zas
Allegra Glashausser
Of Counsel

TO: GEOFFREY S. BERMAN, ESQ.
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007
Attn: **Matthew Laroche and Sidhardha Kamaraju**
Assistant United States Attorneys

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Other Authorities:

STATEMENT OF THE ISSUES

1. Whether the initial March 13, 2017 warrant to search Mr. Schulte's home is invalid under the Fourth Amendment because the warrant application intentionally or recklessly misrepresented numerous material facts, thus requiring suppression of all resulting evidence under *Franks v. Delaware*, 438 U.S. 154 (1978).

2. Whether the initial March 13, 2017 search warrant is invalid under the Fourth Amendment, requiring suppression of all resulting evidence, because the warrant application failed to establish probable cause to believe that evidence of criminal activity would be found at Mr. Schulte's home in New York City.

3. Whether the subsequent April 14, 2017 warrant and May 10, 2017 warrant to search for evidence of child pornography are invalid under the Fourth Amendment because the warrant applications intentionally or recklessly omitted material facts.

4. Whether all of the search warrants in this case are overbroad and insufficiently particularized, thus requiring suppression of the resulting evidence under the Fourth Amendment.

SUMMARY OF ARGUMENT

The FBI obtained and executed nine search warrants in this case between March 13, 2017 and May 17, 2017. But the FBI procured them in flagrant disregard of Mr. Schulte's Fourth Amendment rights by submitting sworn warrant applications that were knowingly or recklessly false and misleading in material respects, or that failed to establish probable cause altogether. The warrants also placed inadequate limitations on the scope of the authorized searches. Accordingly, the warrants are invalid and all resulting evidence must be suppressed.

First, the FBI obtained a warrant on March 13, 2017, to search Mr. Schulte's home in New York City for evidence he stole classified information more than a year earlier, on March 7–8, 2016, and thereafter disclosed it to WikiLeaks by some unidentified means and at some unidentified time. But the warrant application contained numerous false statements (including misleading omissions) that grossly exaggerated the evidence of probable cause. For example, the FBI represented that (1) the classified information "appear[ed]" to have been stolen over a specific 24-hour period in March 2016; (2) Mr. Schulte was "one of only three employees across the entire CIA" who had authorized access to the information; (3) Mr. Schulte was "the only one" of these three employees who was not publicly identified by WikiLeaks; and (4) Mr. Schulte had a perfect opportunity to steal the information without detection because other employees who were normally able to observe him at his desk were away from the office when the information was supposedly taken. In fact, as the government has since conceded, these assertions (and many others) were simply not true. The sheer number and importance of the untrue statements indicate that the FBI made them recklessly or intentionally, warranting suppression. At a minimum, the Court should convene a *Franks* hearing because Mr. Schulte has made "a 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." *United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008). *See* Point I, *infra*.

The initial warrant application is invalid for an additional reason: it failed to establish the necessary nexus between the alleged offenses and Mr. Schulte's home in New York City. Though the warrant application contained a generalized, boilerplate allegation that people who steal classified information tend to use computers and keep computers in their homes, such a

conclusory statement—unconnected to any particular facts about this case—failed to establish probable cause to believe that Mr. Schulte himself even possessed a home computer, much less that it was likely to contain information about the alleged theft of CIA information a full year earlier. And since the warrant application did not allege even a minimal factual connection between the offenses and Mr. Schulte's home, the good-faith exception to the exclusionary rule is inapplicable. *See* Point II, *infra*.

Further, the FBI improperly procured subsequent warrants on April 14, 2017, and May 10, 2017, to search Mr. Schulte's devices for evidence of child pornography. The basis for these warrants was unusually thin—and highly misleading. The FBI represented that it had found a single "photograph" or image on Mr. Schulte's "desktop computer" that "appear[ed] to depict child pornography." But, even assuming the image did in fact "appear" to depict child pornography, the affidavits failed to disclose that (1) the image was actually found in a special, inaccessible area of the computer known as the "page file"; (2) the image bore no indicia of when or how it came to be on the computer; and (3) about 20 percent of the image was blacked out. These omissions were important because the presence of a single, undated, and partially blacked out image in a computer's page file reveals nothing about whether Mr. Schulte ever saw it, intentionally downloaded it, or knowingly possessed it. So, once the omissions are corrected, no probable cause for the child pornography warrants would have existed. The omissions thus suggest a reckless or intentional effort to mislead. Accordingly, the omissions were material, the search warrants for child pornography are void under *Franks*, the good-faith exception does not apply, and the recovered evidence must be suppressed. *See* Point III, *infra*.

Finally, all of the search warrants at issue in this case authorized sweeping searches of Mr. Schulte's electronic devices and online accounts without providing adequate limitations. Thus,

the warrants are unconstitutionally overbroad and insufficiently particularized, and all resulting evidence should be suppressed. *See* Point IV, *infra*.

STATEMENT OF FACTS

On March 7, 2017, WikiLeaks published classified documents allegedly stolen from the CIA. Within days, the FBI targeted Joshua Adam Schulte, a then 28-year-old former CIA software engineer with a history of public service and no criminal record, as the suspected source of the classified documents. At the time, Mr. Schulte was living in New York City and working for Bloomberg L.P.

The initial March 13, 2017 warrant application and search of Mr. Schulte's home

On March 13, 2017, Special Agent Jeff D. Donaldson of the FBI applied in the Southern District of New York for a warrant to search Mr. Schulte's New York City apartment without his knowledge for evidence he was involved in the theft and disclosure of the classified information published by WikiLeaks (the "Classified Information Offenses"). Donaldson filed a supporting affidavit, dated March 13, 2017, claiming probable cause to believe that Mr. Schulte was the culprit.

The affidavit asserted that the classified information "appear[ed] to have been stolen" from the CIA "between the night of March 7, 2016 and the night of March 8, 2016." 3/13/17 Aff.[1] ¶ 8(c). This time frame was important, the affidavit said, for several reasons. First, the affidavit

[1] "3/13/17 Aff." refers to the Affidavit of Jeff D. Donaldson, executed March 13, 2017. "3/14/17 Aff." refers to the Affidavit of Jeff D. Donaldson, executed March 14, 2017. "4/10/17 Aff." refers to the Affidavit of Richard J. Evanchec, executed April 10, 2017. "5/10/17 Aff." refers to the Affidavit of Garrett L. Igo, executed May 10, 2017. "5/17/17 Aff." refers to the Affidavit of Jeff D. Donaldson, executed May 17, 2017. Copies of these affidavits are annexed as exhibits to the Declaration of Sabrina P. Shroff, executed July 3, 2019 ("Shroff Decl."). "Bellovin Decl." refers to the Declaration of Steven M. Bellovin, Ph.D., in Support of Suppression, executed June 28, 2019.

claimed that the classified information "was publicly released by WikiLeaks exactly one year to the day (March 7, 2017)" after it was likely stolen from the CIA (March 7, 2016). 3/13/17 Aff. ¶ 8(d).

Moreover, the affidavit claimed that, in March 2016, Mr. Schulte "was one of only three CIA employees throughout the entire CIA who had authorized access to the CIA Group's Back-Up Server from which the Classified Information was likely copied." 3/13/17 Aff. ¶ 12(b). And the affidavit said that, while the classified information published by WikiLeaks appeared to contain the "names or pseudonyms" of multiple CIA employees—"including two of the three" CIA employees with authorized access to the server from which the classified information was likely taken—Mr. Schulte "was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks's publication of the Classified Information." 3/13/17 Aff. ¶ 12(b).

The affidavit also suggested that Mr. Schulte had a perfect opportunity to steal the information between March 7, 2016, and March 8, 2016. Agent Donaldson averred that, on March 8, 2016, the CIA group in which Mr. Schulte worked held "an office management retreat for many of its senior and midlevel managers," "including some to whom [Mr.] Schulte reported"—but Mr. Schulte did not attend; instead, he remained at work at his CIA office. 3/13/17 Aff. ¶ 13(a)–(b). The affidavit indicated that Mr. Schulte's workspace was "set up such that only three other CIA Group employees … could see what he was doing at his desk." 3/13/17 Aff. ¶ 13(c). But "[a]t least two of those three employees were at the offsite management retreat on March 8, 2016"—supposedly giving Mr. Schulte an ideal opportunity to access and steal the CIA information without fear of detection. 3/13/17 Aff. ¶ 13(c)-(d).

The affidavit also portrayed Mr. Schulte as a disgruntled former CIA employee with a motive to retaliate against the CIA by stealing and disclosing the classified information. And it indicated that Mr. Schulte had a history of violating rules concerning accessing computers and handling classified information. The affidavit stated, for example, that "on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN [Local Area Network] and reinstated his own administrator privileges." 3/13/17 Aff. ¶ 15.

The affidavit also sought—in just two sentences—to establish probable cause to believe that evidence of criminal activity would be found in Mr. Schulte's New York City apartment. Agent Donaldson stated: "Based on my training and experience, I know that individuals who are involved in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials use computers and other electronic devices in furtherance of their criminal activities. Based on my training and experience, I also know that individuals typically keep their computers and other electronic devices in their homes." 3/13/17 Aff. ¶ 22.

As demonstrated in Point I, *infra*, and as a hearing will confirm, Agent Donaldson's March 13, 2017 warrant affidavit was replete with false and misleading information. Among other inaccuracies, many of which the government has already admitted, the classified information was likely *not* stolen over the March 7–8, 2016 time frame; Mr. Schulte was *not* "one of only three employees" with authorized access to the information; his identity *was* publicly disclosed by WikiLeaks; and he was *not* the disgruntled and disobedient employee portrayed by Agent Donaldson.

The magistrate, unaware of the affidavit's many misstatements and inaccuracies, signed the warrant on March 13, 2017. It broadly authorized the FBI to conduct a covert search of Mr.

Schulte's apartment, including any electronic storage devices that might be found there, without any restrictions on the time period to be searched. *See* Attachment "A" to the 3/13/17 Search and Seizure Warrant.

The second warrant application and home search: March 14, 2017

When the FBI executed the initial search warrant (on the afternoon of March 13, 2017), they discovered that Mr. Schulte possessed an array of electronic devices in his home and realized it would be "impractical" to search all of them covertly. *See* 3/14/17 Aff. ¶ 9. Indeed, the FBI discovered over 150 items, amounting to well over 12.74 terabytes of data, including desktop computers, servers, numerous external hard drives, "thumb" drives, CDs, DVDs, floppy disks, cell phones, gaming systems, tablets, e-readers, a camera, and MP3 players. Accordingly, the next day, the FBI sought a second warrant authorizing the government to remove all of the devices from Mr. Schulte's apartment and search them for evidence relating to the Classified Information Offenses. The warrant application was materially identical to the first one (except the FBI now knew about all the devices in Mr. Schulte's apartment).

The magistrate issued the second warrant on March 14, 2017, and the FBI executed it the same day. During this second search, the agents spoke to Mr. Schulte and seized his passport to prevent him from going on vacation to Cancun, Mexico, with his younger brother, but did not arrest him. Mr. Schulte cooperated, agreed to be interviewed numerous times, and consistently denied any involvement in the crimes.

The March 14, 2017 warrants for Mr. Schulte's account information with Google, Reddit, and GitHub

On March 14, 2017, the FBI also sought and obtained three additional warrants to seize and search records of Mr. Schulte's accounts with Google, Reddit, and GitHub for evidence relating to the Classified Information Offenses. *See* Shroff Decl. Exh. C (collectively, "Online Account

Warrants"). The scope of these warrants was exceedingly broad. Though the Classified Information Offenses allegedly took place beginning in March 2016, Google was directed to produce "all" information associated with Mr. Schulte's 11-year-old Gmail account, including his entire search history; all photos; "all files and folders;" "[a]ll records, voicemails, text messages, and other data associated with Google Voice;" "[a]ll" Google Wallet information; "all" YouTube videos, comments, or private messages; "[a]ll emails," even those that were drafts; and all contacts. Shroff Decl. Exh. C (JAS_128-30). The Reddit and GitHub warrants similarly directed the production of everything those companies had relating to Mr. Schulte. *Id.* (JAS_ l34-35; 139-40). The warrants authorized the government to search the information for evidence relating to the Classified Information Offenses.

The child pornography warrants: April 14, 2017, May 10, 2017, and May 17, 2017

On April 7, 2017, while purportedly searching Mr. Schulte's devices only for evidence relating to the Classified Information Offenses, the FBI found something else: a single purported "photograph" or image that supposedly "appear[ed] to" depict child pornography. The FBI contacted the prosecutors, who advised the FBI to seek a new warrant permitting them to search Mr. Schulte's devices for evidence relating to child pornography. *See* 4/14/17 Aff. ¶ 3.

But the FBI decided not to await the warrant. Instead, they began searching for evidence of child pornography. Specifically, the agents who had been searching Mr. Schulte's account records with Google, Reddit, and GitHub pursuant to the Online Account Warrants decided to exceed the scope of those warrants. Those warrants authorized the agents to search only for evidence relating to the Classified Information Offenses. But the agents nevertheless proceeded to search Mr. Schulte's online accounts for evidence related to child pornography. *See* 5/10/17 Aff. ¶ 14 n.6. As a result of those unauthorized searches, the FBI learned that, in 2011 and 2012,

Mr. Schulte had "apparently" searched on Google (a) three times for "child pornography"; (b) for "movie where father videos daughter and friend sex [sic]" and "movie where father videos child porn"; and (c) for "female teenage body by year." 4/10/17 Aff. ¶ 15.[2]

Based on these Google searches and the single image found on April 7, 2017, the FBI applied on April 14, 2017, for a warrant to search all of Mr. Schulte's devices for evidence relating to child pornography. The supporting affidavit was provided by FBI Special Agent Richard J. Evanchec. He averred that, on or about April 7, 2017, "a photograph was discovered on [Mr. Schulte's] desktop computer … that appears to depict child pornography." 4/14/17 Aff. ¶ 13. The agent did not provide the supposed "photograph" to the magistrate. Instead, the agent stated that he had spoken to other FBI agents who, in turn, had spoken to an agent assigned to the Crimes Against Children Squad (CACS) and that "the CACS Agent believe[d] the CP Picture depicts 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—oral sex around the child's buttocks." 4/14/17 Aff. ¶ 14.

The affidavit also included the results of the unauthorized FBI searches of Mr. Schulte's Google accounts for evidence relating to child pornography, discussed above. The affidavit

[2] In applying for the April 10, 2017 warrant, the FBI took these searches out of context to make them appear sinister. In fact, they were innocuous. As shown by his Internet chats from the surrounding time, Mr. Schulte was trying to recall the name of *The Butterfly Effect*, a mainstream Hollywood movie in which the "father videos [his] daughter and friend [having] sex"; the very next search (only 23 seconds later) was for "movie where guy keeps going back in time to relive past." Shroff Decl. Exhs. D, E (JAS_000024, JAS_000028). In any event, because the FBI uncovered these Google searches illegally (i.e., by exceeding the scope of the Online Account Warrants), they should not have been included in the April 10 warrant application, as the subsequent May 10, 2017 warrant application effectively acknowledged. *See* 5/10/17 Aff. ¶ 14 n.6.

claimed, based on this evidence, that Mr. Schulte "appear[ed] to have searched the Internet for child pornography in or about 2011 and in or about 2012." 4/14/17 Aff. ¶ 15.

The affidavit also claimed that the FBI had found the single supposed "CP" image on Mr. Schulte's "desktop computer." 4/14/17 Aff. ¶ 13. In fact, the agents found the image in a special, inaccessible area of the computer known as the "page file." The image's presence there, standing alone, did "not provide a basis for concluding that [it] was ever knowingly accessed, received, possessed, or even seen by" Mr. Schulte. *See* Bellovin Decl. ¶¶ 7, 10–11. The affidavit also failed to disclose to the magistrate that about 20 percent of the image was blacked out—a fact consistent with the image having been present on the computer without Mr. Schulte's knowledge. *See id.* ¶ 12.

Pursuant to the April 14, 2017 and May 10, 2017 child pornography warrants, the FBI searched Mr. Schulte's devices and allegedly found additional images of child pornography.

Finally, on May 17, 2017, Agent Donaldson applied for and obtained a warrant to search Mr. Schulte's Google account for evidence relating to the Classified Information Offenses, child pornography, and copyright infringement.[3]

The charges

On September 6, 2017, six months after the unauthorized WikiLeaks publication, the government indicted Mr. Schulte, charging him solely with three counts relating to child pornography. Nine months later, in June 2018, the government filed a superseding indictment, adding charges relating to the theft and disclosure of classified information, as well as one count of copyright infringement. On October 31, 2018, the government filed a second superseding

[3] The FBI also obtained a warrant on May 5, 2017, to seize and search information from Mr. Schulte's employer at the time, Bloomberg L.P.

indictment adding two additional counts for offenses Mr. Schulte allegedly committed while incarcerated.

The *Brady* letter

On September 28, 2018, in a letter to defense counsel pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963),[4] the government admitted, *inter alia*, that the initial March 13, 2017 search warrant affidavit was inaccurate in many important respects. Indeed, the government appears to have abandoned the central themes of the March 13 affidavit: namely, that the CIA information was likely stolen on March 7–8, 2016, that Mr. Schulte was essentially "one of only three people" across the entire CIA who could have taken it, and that WikiLeaks's supposed effort to conceal his identity was telltale evidence of his culpability. *See* Shroff Decl. Exh. F (*Brady* letter at 2–8); *see also* Shroff Decl. Exh. G (Bill of Particulars) (now claiming that the information was stolen around April 20, 2016).

The *Brady* letter thus acknowledged that the March 13 affidavit had falsely stated that the classified information was likely stolen on March 7–8, 2016. The government further admitted that the number of people who had access to the classified information was significantly larger than Agent Donaldson had led the magistrate judge to believe. For example, the March 13 affidavit stated many times that Mr. Schulte was "one of only three people" who had authorized access to the "specific portion" "of the network" where the government believed the stolen information was stored. But, in truth, "at least" five employees—and perhaps dozens of others—had access to that portion of the network. *See* Shroff Decl. Exh. F (*Brady* letter) at 2.

[4] *Brady* holds that the prosecution has a constitutional duty to disclose evidence favorable to the accused when such evidence is material to guilt or punishment. *See Brady*, 373 U.S. at 87.

The *Brady* letter also acknowledged numerous misstatements in the March 13 affidavit regarding Mr. Schulte's alleged unauthorized access to CIA projects and systems in April 2016. *See* Shroff Decl. Exh. F at 7–8.

Additionally, the affidavit misstated the mechanics of how the classification information was supposedly taken. For example, the affidavit claimed that the classified information was apparently copied from an automated daily back-up file, but the *Brady* letter stated that the script used to back up files to the server had to be manually initiated. *See* Shroff Decl. Exh. F at 6.

Finally, the *Brady* letter explained that a key aspect of the affidavit's narrative—that Mr. Schulte was the likely culprit because WikiLeaks suspiciously did not publicly disclose his identity—was false. Mr. Schulte's identity (specifically, his computer username "SchulJo") was mentioned numerous times by WikiLeaks, as a simple word-search of the WikiLeaks publication would have shown. *See* Shroff Decl. Exh. F at 7.

ARGUMENT

Point I

The initial March 13, 2017 search warrant is void because it contained deliberate or reckless misstatements or omissions of material fact. Accordingly, the good-faith exception to the exclusionary rule does not apply, and all resulting evidence must be suppressed. At a minimum, an evidentiary hearing is required.

The initial March 13, 2017 search warrant application contained numerous misstatements, some of which were repeated numerous times. These misstatements, many of which the government has now acknowledged, were crucial to the appearance of probable cause. For example, the number of people who had authorized access to the classified information disclosed by WikiLeaks was not three but at least five, and potentially many more. The information was not stolen on a special day when Mr. Schulte was the only person with unfettered access at work, but on a normal day during which any number of other CIA employees could have stolen the information. And the FBI falsely suggested Schulte must be the culprit because, while WikiLeaks disclosed the names or pseudonyms of other CIA employees, it suspiciously did not publish his identity. In fact, WikiLeaks *did* disclose Mr. Schulte's identity, just as it disclosed the identities of other CIA employees who had access to the stolen information. Once these falsehoods are corrected, the existence of probable cause against Mr. Schulte vanishes.

Moreover, the number and significance of the misstatements indicate at least a reckless disregard for the truth. All of the misstatements worked in the government's favor by artificially bolstering the evidence of probable cause. Thus, recklessness may be inferred. *See United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. l996) ("recklessness may be inferred" where false or omitted information was "'clearly critical' to assessing the legality of a search") (internal citation omitted); *United States v. Lahey*, 967 F. Supp. 2d 698, 723 (S.D.N.Y. 2013) (Karas, J.) (inferring

recklessness under *Franks* where a series of related omissions "dr[o]ve in the same direction" of buttressing probable cause). Accordingly, the Court needs to conduct a *Franks* hearing. *See, e.g.*, *United States v. Padilla*, 986 F. Supp. 163, 168–69 (S.D.N.Y. 1997) (*Franks* hearing required where government "concede[d] that the bulk of the information contained in the complaint was false"); *see also United States v. Chesher*, 678 F.2d 1353, 1362 (9th Cir. 1982) (denial of *Franks* hearing was reversible error: "Clear proof is not required [to obtain a *Franks* hearing]—for it is at the evidentiary hearing itself that the defendant, aided by live testimony and cross-examination, must prove actual recklessness or deliberate falsity.").

A. A warrant is void when procured through deliberate or reckless misrepresentations of material fact.

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

For a warrant to issue, a magistrate must 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); *see also United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015).

In this case, the FBI obtained a warrant on March 13, 2017, to search Mr. Schulte's home, but that warrant does not insulate the search from Fourth Amendment scrutiny. A defendant is entitled to a hearing under *Franks* if he makes 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 finding of probable cause." *United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008) (quoting *Franks*, 438 U.S. at 155–56).

The defense should make an "offer of proof," "point out specifically the portion of the warrant affidavit that is claimed to be false," and provide "a statement of supporting reasons." *Franks*, 438 U.S. at 171. "Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained." *Id.*

If the hearing demonstrates that the affidavit included deliberate falsehoods or statements made with reckless disregard for the truth, and that, "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *Franks*, 438 U.S. at 156; *see also United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013). Moreover, *Franks* protects against misleading *omissions* as well as affirmative *misstatements. See United States v. Awadallah*, 349 F.3d 42, 68 (2d Cir. 2003); *United States v. Levasseur*, 816 F.2d 37, 43 (2d Cir. 1987).

An agent "recklessly disregards" the truth in the *Franks* context when he or she "makes allegations while entertaining serious doubts about the[ir] accuracy," *see United States v. Vilar*, 2007 WL 1075041, at *26 (S.D.N.Y. Apr. 4, 2007) (collecting authorities), or while "aware of a high probability" that the allegations "might be false." *Varnish v. Best Medium Pub. Co.*, 405 F.2d 608, 623 (2d Cir. 1968). An omission satisfies the *Franks* standard if it was "'designed to mislead,' or … was 'made in reckless disregard of whether [it] would mislead' the magistrate." *Rajaratnam*, 719 F.3d at 154 (quoting *Awadallah*, 349 F.3d at 68).

B. The initial March 13, 2017 warrant is void under *Franks*.

The *Franks* standard for suppression is satisfied here. The government has already confessed in its *Brady* letter that many of Agent Donaldson's sworn statements in his initial March 13, 2017 affidavit were not true. And an evidentiary hearing will show that many

additional statements were untrue or misleading, that they were material to the probable cause determination, and that they were made in an intentional or reckless effort to mislead.

1. The affidavit contained numerous false or misleading statements.

Agent Donaldson swore that all of the following statements were true:

- Only employees of Mr. Schulte's CIA group "had access to the computer network on which the Classified Information that was stolen from the CIA Group's computer network was stored." 3/13/17 Aff. ¶ 8(b).
- Only three of the "approximately 200 people who worked for the CIA Group had access to the specific portion of the Group's computer network on which the Classified Information was likely stored." *Id.* ¶ 5. This claim is repeated numerous times. *See id.* ¶¶ 8(b), 12, 12(a), 12(b), 12(b)(iii), 12(c), 13(d).
- 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." *Id.* ¶ 8(c). This assertion appears repeatedly. *See id.* ¶¶ 8(c)(i), 8(c)(ii), 8(d), 10(a), 10(e), 13.
- The Classified Information "originated in a specific isolated local area computer network ('LAN') used exclusively by the CIA Group." *Id.* ¶ 9.
- "In and around March 2016, in total less than 200 people had access to the CIA Group's LAN on which the Classified Information was stored." *Id.*
- "The fact that the Classified Information contains numerous iterations (or snapshots) of the similar or same data, distinguished by date, is strongly supportive

of the fact that the Classified Information was taken from the CIA Group's Back-Up Server." *Id.* ¶ 10(d).

- "The CIA Group's 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." *Id.* ¶ 11.
- "In approximately March 2016 … only three CIA employees were designated Systems Administrators with access to the CIA Group's Back-Up Server." *Id.* ¶ 12(b); *see also id.* ¶ 13(d).
- Mr. Schulte's "name … was not apparently published in the Classified Information" released by WikiLeaks. *Id.* ¶ 12(b)(ii).
- Mr. Schulte "was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks's publication of the Classified Information." *Id.* ¶ 12(b)(iii).
- "On or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges." 3/13/17 Aff. ¶ 15.

In reality, as a hearing will demonstrate, these statements, and many others in the affidavit, were inaccurate, misleading, or downright false. And this offer of proof is far from conclusory: it is supported by the government's *Brady* letter, the FBI's own official reports of witness statements ("302s"), and other documents produced by the government in discovery (*see* Classified Addendum to this Memorandum, Shroff Decl. Exh. K).

2. The false or misleading statements were material because they were necessary to the probable cause determination.

The misstatements were material because after "setting aside the falsehoods in the application," the "untainted portions of the application" did not "suffice to support" a probable cause finding. *Rajaratnam*, 719 F.3d at 146 (citations omitted).

This case is thus unlike *Rajaratnam*. There, the Second Circuit held that suppression was not warranted because the record—which included a *Franks* hearing—established "that fully disclosing the details of th[e] investigation would only have *strengthened* the wiretap application[]." *Rajaratnam*, 719 F.3d at 155. The opposite is true here. Disclosing the truth would have fatally *weakened* the warrant application. And since the entire case against Mr. Schulte, even with the falsehoods, was circumstantial, the "hypothetical corrected affidavit" would have provided "a thin reed on which to base a search." *Lahey*, 967 F. Supp. 2d at 724.

Indeed, the false or misleading information was the foundation of the magistrate's probable cause determination. The affidavit swore—falsely—that Mr. Schulte was one of only three people "across the entire CIA" with the access and opportunity to take the classified information. It swore—falsely—that only three people had access to the CIA server from which the information was likely stolen, and that only Mr. Schulte and one other person were in the office the day the information was taken. It also swore—falsely—that WikiLeaks suspiciously did not disclose Mr. Schulte's identity, while it did disclose the identities of other people who had access to the stolen information.

Without these false allegations, only four main allegations remain: First, the affidavit claimed that Mr. Schulte had a sophisticated computer skill set that enabled him to "write code designed to clandestinely copy data from computers,'' 3/13/17 Aff. ¶ 12(a)(iii); 3/14/17 Aff. ¶ 18(a)(iii). But so did everyone he worked with—that was part of their training and jobs.

Second, the affidavit alleged that Mr. Schulte's administrator privileges for a project were adjusted in April and May 2016. *See* 3/13/17 Aff. ¶¶ 14–15. But this information was not incriminatory—the affidavit did not claim that the privileges were changed because of any misconduct; they were changed only because Mr. Schulte was transferred to a different group within the CIA.

Third, the affidavit alleged that Mr. Schulte had resigned from the CIA after expressing dissatisfaction with the way the CIA handled his reports about a conflict with a colleague and security flaws in the computer network. But these allegations surely did not constitute probable cause to believe he committed federal crimes by stealing and leaking classified information.

Fourth, as the affidavit noted, Mr. Schulte asked former CIA colleagues about the status of the investigation into the WikiLeaks publication. However, his interest in the matter was perfectly normal given that he used to work at the CIA. 3/13/17 Aff. ¶ 20(d).

Given the absence of probable cause once the false and misleading statements are excised or corrected, those statements were material. *See, e.g.*, *Reilly*, 76 F.3d at 1280 (omissions were material where affidavit gave "no description" of the area where marijuana plants were seen and such description "was crucial"); *Lahey*, 967 F. Supp. 2d at 724–27; *United States v. Big Apple Bag* Co., 306 F. Supp. 2d 331, 334–37, *on reconsideration in part*, 317 F. Supp. 2d 181 (E.D.N.Y. 2004) (no probable cause to believe drug paraphernalia was located at warehouse when the affidavit, *inter alia*, falsely stated there were thousands of items used to measure cocaine when there were only three); *United States v. Roman*, 311 F. Supp. 3d 427, 439–41 (D. Mass. 2018); *see also Padilla*, 986 F. Supp. at 168–69 (*Franks* hearing required where there was "a strong likelihood that this complaint failed to establish probable cause in the absence of the false material").

3. The false or misleading statements were made intentionally or recklessly.

Though "misstatements or omissions caused by negligence or innocent mistakes do not warrant suppression," *United States v. Lambus*, 897 F.3d 368, 399 (2d Cir. 2018), a hearing will demonstrate that the statements here were not made through mere carelessness. The sheer number and importance of the misstatements strongly suggest that the FBI acted with at least reckless disregard for the truth. *See Lahey*, 967 F. Supp. 2d at 723; *see also Reilly*, 76 F.3d at 1280 (noting that recklessness "may be inferred when omitted information was clearly critical to assessing the legality of the search") (internal quotation marks omitted). "While the omission of each individual fact may not necessarily lead to the conclusion that [the affiant] acted with reckless disregard for the truth, *the cumulative effect* of all of the omissions was to eliminate nearly every indicator detracting from [probable cause]." *Lahey*, 967 F. Supp. 2d at 723 (quoting *United States v. Simmons*, 771 F. Supp. 2d 908, 918 (N.D. Ill. 2011)) (emphasis added). *See also Reilly*, 76 F.3d at 1280 (inferring recklessness where affiants "fail[ed] to provide all potentially adverse information" in warrant application); *Roman*, 31 l F. Supp. 3d at 429 (finding "the Government committed a series of easily avoidable errors which, combined with the admittedly high risk of the harm … amounted to a reckless disregard for the truth"); *United States v. Harris*, 464 F.3d 733, 737 (7th Cir. 2006) (remanding for *Franks* hearing where district court found that the affidavit's omissions, "both individually and in their cumulative effect, suggest an intentional design to create an incorrect or at least misleading impression that the evidence relied upon to obtain the warrant was more current than it actually was"). Indeed, the aggregate effect of the FBI's numerous misstatements was even greater here than in *Lahey*, *Roman*, and *Simmons*. The effect of each of the misstatements "dr[o]ve in the same direction: establishing a connection"

between Mr. Schulte and the theft of the classified information, "which connection the fuller evidence did not support." *Lahey*, 967 F. Supp. 2d at 723.

Moreover, numerous documents in the classified discovery contradict the statements included in the initial warrant affidavit. These contradictions suggest—and an evidentiary hearing will confirm—that Agent Donaldson and his colleagues recklessly or intentionally disregarded the truth in seeking the warrant. *See, e.g., Big Apple Bag Co.*, 306 F. Supp. 2d at 334–35 (granting suppression where warrant affidavit conflicted with FBI report about the presence of crack pipes in a warehouse); *United States v. Castellanos*, 820 F. Supp. 80, 84–86 (S.D.N.Y. 1993) (granting suppression where affiant included information regarding defendant's meeting with confidential informant that was not in Drug Enforcement Administration report and that conflicted with informant's testimony).

C. Suppression is warranted.

Because the initial March 13, 2017 search warrant is void under *Franks*, the good-faith exception to the exclusionary rule does not apply. *See United States v. Leon*, 468 U.S. 897, 923 (1984); *Reilly*, 76 F.3d at 1280–81. Accordingly, the Court should suppress all evidence that was obtained, directly or indirectly, as a result of the initial warrant. *See Wong Sun v. United States*, 371 U.S. 471, 484–85 (1963); *Young v. Conway*, 698 F.3d 69, 77 (2d Cir. 2012). And since probable cause for all the subsequent search warrants depended on evidence obtained pursuant to the invalid initial warrant, the subsequent warrants (and the resulting searches) are "tainted" and therefore invalid as well. *See United States v. Trzaska*, 111 F.3d 1019, 1026 (2d Cir. 1997) (suppression is required unless subsequent warrant affidavit, "excised of the tainted evidence," establishes probable cause); *United States v. Reyes*, 922 F. Supp. 818, 831 (S.D.N.Y. 1996) (suppressing evidence seized during second

search of storage facility where warrant application merely incorporated prior search warrant's affidavit and results of that search, because first warrant lacked probable cause); *see also United States v. Calhoun*, 2017 WL 1078634, at *13 (D. Conn. Mar. 21, 2017) (suppressing evidence where "tainted evidence play[ed] a central role" in providing probable cause to search defendant's home); *Reilly*, 76 F.3d at 1280 (declining to apply good-faith exception when "issuance of the warrant was itself premised on material obtained in a prior search that today's holding makes clear was illegal").

* * *

In this situation, where the government has already admitted to numerous, material errors in the warrant application, and the FBI's own reports indicate that it disregarded accurate information, the Court should conclude that the agents acted at least recklessly, and suppress the resulting evidence. At the very least, Mr. Schulte has made a "substantial preliminary showing" sufficient to require an evidentiary hearing. *See, e.g., United States v. Koschtschuk*, 2011 WL 867569, at *5 (W.D.N.Y. Mar. 10, 2011); *United States v. Benacquista*, 2009 WL 1651458, at *7 (W.D.N.Y. June 8, 2009); *United States v. Westover*, 812 F. Supp. 38, 39 (D. Vt. 1993); *Big Apple Bag Co.*, 317 F. Supp. 2d at 181; *Castellanos*, 820 F. Supp. 80, 82 (S.D.N.Y. 1993).

Point II

The initial warrant to search Mr. Schulte's New York City home is invalid, and the good-faith exception to the exclusionary rule does not apply, because the supporting affidavit failed to establish even a minimal factual nexus between the alleged offenses and the home.

The initial March 13, 2017 warrant is invalid for an independent reason: Agent Donaldson's supporting affidavit did not establish probable cause to believe that evidence of criminal activity would be found in Mr. Schulte's New York City home in March 2017.

The Fourth Amendment was adopted largely to "prevent … 'general, exploratory rummaging in a person's belongings' and the attendant privacy violations." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). At "the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Silverman v. United States*, 365 U.S. 505, 511 (1961).

Accordingly, "[t]o establish probable cause to search a residence, two factual showings are necessary—first, that a crime was committed, and second, that there is probable cause to believe that *evidence of such crime is located at the residence." United States v. Travisano*, 724 F.2d 341, 345 (2d Cir. 1983) (emphasis added). The second factual determination asks whether based on "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, 214 (1983); *see also Raymonda*, 780 F.3d at 113. And while the magistrate's probable cause determination is entitled to deference, such deference "is not boundless." *Leon*, 468 U.S. at 914. "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions" of others, or an "improper analysis of the totality of the circumstances." *Id.* at 915; *Massachusetts v. Upton*, 466 U.S. 727, 734 (1984); *Gates*, 462 U.S. at 239. And probable cause must emerge from the facts set forth in the warrant affidavit itself. *See id.* at 238 (probable cause determinations depend on "all the circumstances set forth in the affidavit"); *United States v. Brooks*, 594 F.3d 488, 492 (6th Cir. 2010) ("When determining whether an affidavit establishes probable cause, we look only to the four corners of the affidavit; information known to the officer but not conveyed to the magistrate is irrelevant.").

Here, the March 13, 2017 warrant application contained no facts connecting the alleged crimes to Mr. Schulte's New York City home. Instead, Agent Donaldson merely offered a conclusory assertion, supposedly based on his "training and experience," that people who steal or disclose classified information tend to use computers or other electronic devices and keep such devices in their homes. 3/13/17 Aff. ¶ 22. But this kind of general statement is precisely the type of "conclusory statement that gives the magistrate virtually no basis at all for making a judgment regarding probable cause." *Gates*, 462 U.S. at 239. Thus, the affidavit did not supply probable cause to search Mr. Schulte's New York City apartment, and the good-faith exception to the exclusionary rule does not apply.

A. The March 13 affidavit contained no factual allegations connecting the alleged offenses to Mr. Schulte's New York City home.

The absence of facts connecting the theft or disclosure of classified information to Mr. Schulte's New York City home is significant because "a determination of probable cause to search is not the same as a determination that there is, at the same time, probable cause to arrest, or vice versa." *United States v. Pabon*, 871 F.3d 164, 181 (2d Cir. 2017); *see also United States v. Burton*, 288 F.3d 91, 103 (3d Cir. 2002) ("[P]robable cause to arrest does not automatically provide probable cause to search the arrestee's home."); *United States v. Santarsiero*, 566 F. Supp. 536, 538 (S.D.N.Y. 1983) ("Probable cause to arrest an individual does not, in and of itself, provide probable cause to search that person's home or car."). Rather, probable cause to search must be based on "a sufficient nexus between the criminal activities alleged" and the location or items to be searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004).

This nexus requirement is particularly important here, for two reasons. First, the government sought to search Mr. Schulte's home, a place at "the very core" of the Fourth Amendment's protections. *Silverman*, 365 U.S. at 511. Second, the government sought to search

every electronic device he might have, thereby examining virtually every aspect of his personal life. *See Riley v. California*, 134 S. Ct. 2473, 2489–90 (2014) (explaining that even microcomputers, such as cellphones, have "immense storage capacity" that may contain "every piece of mail [people] have received for the past several months, every picture they have taken, or every book or article they have read," which can allow the "sum of an individual's private life [to] be reconstructed"). Accordingly, the search "involve[d] the prospect of an especially invasive search of an especially protected place." *United States v. Griffith*, 867 F.3d 1265, 1272 (D.C. Cir. 2017); *see also United States v. Mitchell*, 565 F.3d 1347, 1351–52 (11th Cir. 2009) (noting the heightened privacy interests in personal computers).

Yet, despite these heightened Fourth Amendment concerns, the March 13, 2017 warrant affidavit provided no factual nexus connecting Mr. Schulte's New York City residence to any offense. The affidavit alleged that classified information was likely stolen from the CIA in Virginia in March 2016, when Mr. Schulte was working and living in Virginia. It did not allege how the classified information was taken; it did not discuss, for example, whether it was stolen using a cell phone, laptop computer, computer disk, portable "thumb" drive, or some other device. The affidavit also did not allege any facts to suggest that Mr. Schulte, even in March 2016, possessed a home computer or other device that could be used to extract the classified information; nor did it allege facts suggesting that any such device would be found in his New York apartment a full year later in March 2017. Indeed, the affidavit alleged no facts to indicate that Mr. Schulte even *had* a computer or other electronic storage device, either in his former Virginia home or in his New York City apartment. *Cf. United States v. Harding*, 273 F. Supp. 2d 411, 416–18 (S.D.N.Y. 2003) (Kaplan, J.) (nexus to home was established where warrant affidavit indicated that defendant had purchased desktop and laptop computers for use at home,

subscribed to Internet access in his home, and accessed the Internet from home the day before the warrant was sought); *United States v. Vosburgh*, 602 F.3d 512, 526–27 (3d Cir. 2010) (nexus to home was established where affidavit explained, *inter alia*, that downloading of child pornography was traced to specific Internet Protocol (IP) address associated with defendant's apartment).

Even if the affidavit had supplied facts to suggest that Mr. Schulte had a computer or other electronic device in his Virginia home in March 2016, and that such a device was used to commit the Classified Information Offenses, the affidavit contained no facts to support a reasonable inference that incriminating evidence would be found on such a device in his *New York City apartment* in March 2017. On the contrary, given Mr. Schulte's admitted expertise with computers and covert operations, there was every reason to believe he would have deleted or discarded any incriminating evidence long before the WikiLeaks publication on March 7, 2017—and certainly afterwards, when he knew the FBI was investigating the leak but before the FBI applied for a warrant to search his home on March 13, 2017. *See Griffith*, 867 F.3d 1275 (recognizing that '"the opportunities those involved in the crime would have had to remove or destroy [incriminating] items' … is an important consideration when assessing the existence of probable cause") (quoting 2 Wayne R. Lafave, *Search & Seizure* § 3.7(a) (5th ed. 2016)). Thus, probable cause did not exist to search Mr. Schulte's New York apartment. *See, e.g.*, *United States v. Kortright*, No. 10-CR-937 (KMW), 2011 WL 4406352, at *7 (S.D.N.Y. Sept. 13, 2011) (finding no probable cause where "the only factual link in the Affidavit between Defendant's alleged criminal activity and the Apartment is the fact that Defendant resided at the Apartment"); *United States v. Moran*, 349 F. Supp. 2d 425, 477 (N.D.N.Y. 2005) (holding that where "there is no factual connection between the criminal activity … and the residence … there is no basis for

finding probable cause"); *see also Griffith*, 867 F.3d at 1273 ("To justify a search of the apartment … police needed reason to think not only that [defendant] possessed a phone, but also that the device would be located in the home and would contain incriminating evidence about his suspected offense.").

1. *Agent Donaldson's general conclusions based on his "training and experience" were insufficient to establish the requisite nexus to search Mr. Schulte's home.*

The only allegation in the March 13 affidavit that even attempted to tie the alleged crimes to Mr. Schulte's New York apartment was Agent Donaldson's conclusory assertion that, based on his "training and experience, … individuals who are involved in [stealing or disclosing classified information] use computers and other electronic devices in furtherance of their criminal activities," and such "individuals typically keep their computers and other electronic devices in their homes." 3/13/17 Aff. ¶ 22.

But numerous courts—including several in this Circuit[5]—recognize that a law enforcement officer's purported "expert" opinion about how criminals in general behave is, without more, insufficient to establish probable cause to search a suspect's residence, even where there is probable cause to believe he or she engaged in a crime. *See, e.g., Griffith*, 867 F.3d at 1274–75 (police officer's opinion, based on his "training and experience," that gang members often use cell phones and other electronic devices to "share intelligence about their activities," did not justify warrant to search suspected gang member's home for such devices in connection with murder investigation); *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir. 1994) (an officer's

[5] The Second Circuit itself warned decades ago that a government agent's expert opinion, "standing alone, might not be sufficient to establish a link between the [defendants'] current homes and their prior criminal activity." *United States v. Benevento*, 836 F.2d 60, 71 (2d Cir. 1987) (citing *United States v. Gomez*, 652 F. Supp. 461, 463 (E.D.N.Y. 1987)), *abrogated on other grounds by United States v. Indelicato*, 865 F.2d 1370 (2d Cir. 1989).

training and experience "cannot substitute for the lack of evidentiary nexus"); *Kortright*, 2011 WL 4406352, at *7 (holding that "stale information (one year old) that Defendant dealt drugs on a handful of occasions, combined with … an expert opinion that drug dealers typically keep drugs in their homes, is not enough to establish probable cause to search the Apartment"); *United States v. Guzman*, No. SS 97-CR-786 (SAS), 1998 WL 61850, at *3–4 (S.D.N.Y. Feb. 13, 1998) (agreeing that "the averments of law enforcement officials concerning general criminal practices, alone, are insufficient to support a finding of probable cause to search the residence of a suspected drug trafficker"); *United States v. Rios*, 881 F. Supp. 772, 776 (D. Conn. 1995) (holding that an agent's "general averments based on her training and experience do not, standing alone, constitute a 'substantial basis' for the issuance of this search warrant"); *Gomez*, 652 F. Supp. at 462 (same).

2. The allegations concerning the theft of CIA information in Virginia in March 2016 were too stale to justify searching Mr. Schulte's home in New York a full year later, in March 2017.

The purported nexus to Mr. Schulte's home was especially inadequate because the alleged basis for the search was stale. Since probable cause must "exist as of the time of the search and not simply as of some time in the past," "the facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and the subsequent search conducted." *United States v. Wagner*, 989 F.2d 69, 75 (2d Cir. 1993). "The two critical factors in determining staleness are the age of the facts alleged and the nature of the conduct alleged to have violated the law." *Raymonda*, 780 F.3d at 114 (internal quotation marks omitted). Additional relevant factors include the nature of the information forming the basis for probable

cause, and the nature of the evidence being sought. *United States v. McGrath*, 622 F.2d 36, 41–42 (2d Cir. 1980).

Here, the relevant factual allegations were too stale to establish probable cause to search Mr. Schulte's New York home on March 13, 2017. First, the affidavit alleged that the classified information was likely copied from a CIA back-up server over a year earlier, on March 7–8, 2016. 3/13/17 Aff. ¶ 8(c). And all the critical facts relating to Mr. Schulte concerned his activities before he resigned from the CIA in November 2016. 3/13/17 Aff. ¶ 19(c).

Moreover, the nature of the crimes at issue—clandestinely copying large quantities of classified information from a CIA server and leaking the information to WikiLeaks—required extraordinarily sophisticated technical ability. Anyone capable of performing such a feat—especially a former CIA software engineer who knew he would likely be a prime suspect—would discard or destroy any incriminating evidence soon after committing the crime. The affidavit itself admitted that Mr. Schulte was a CIA System Administrator with "a skill set that enabled him to write computer code" to perform "clandestine[]" operations. 3/13/17 Aff. ¶ 12(a)(iii). Indeed, Agent Donaldson acknowledged that Mr. Schulte had the ability "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." 3/13/17 Aff. ¶ 37(c).

Thus, this is not like the ordinary case involving business records or child pornography, in which it may be reasonable to infer that incriminating evidence would remain on a computer for an extended period. Rather, the nature of the alleged crimes, the evidence sought, and Mr. Schulte's computer expertise suggest that any incriminating evidence would have been destroyed, discarded, or hidden outside the home. *See Griffith*, 867 F.3d at 1274 (no probable

cause to obtain warrant to search a home for cell phone where crime took place "more than a year" earlier and defendant "had every incentive to cleanse his phone" of incriminating evidence); *see also United States v. Paul*, 692 F. Supp. 186, 193 (S.D.N.Y. 1988) (holding that based on the isolated nature of the alleged extortion, "it is more reasonable to infer that an extortionist would seek to disperse or spend his booty in an attempt to hide it"; thus, information in affidavit was too stale to establish probable cause).

Put simply, given (1) the year-long period between the alleged theft of the classified information (March 2016) and the application for the search warrant (March 2017), (2) Mr. Schulte's acknowledged expertise in computers and covert operations, and (3) his move in November 2016 from Virginia to New York, the affidavit provided no factual basis to conclude that incriminating evidence would likely be found in Mr. Schulte's New York City apartment on March 13, 2017.[6] Thus, no probable cause existed to search his home.

B. The good-faith exception to the exclusionary rule does not apply.

The invalidity of a search warrant does not always require suppressing evidence recovered in its execution. Under the good-faith exception to the exclusionary rule, "evidence seized in reasonable, good-faith reliance on a search warrant" need not be excluded, even if the warrant turns out to have been unsupported by probable cause. *Leon*, 468 U.S. at 905 (citation omitted).

But "[g]ood faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *Reilly*, 76 F.3d at 1280. For the good-faith exception to apply, law enforcement "must reasonably believe that the warrant was based on a valid application of the

[6] Significantly, though the affidavit alleged that WikiLeaks had published the classified information on March 7, 2017, it did not allege when (or how) WikiLeaks acquired the information. The government now says that Mr. Schulte illegally transmitted the information to WikiLeaks in "late April or early May 2016." Shroff Decl. Exh. G, at 2. The government's latest theory confirms that there was no basis to search his home so many months later, in March 2017.

law to the known facts.*"* *Id.* at 1280. That means the exception does not apply where the warrant application contains no facts to establish even a "minimal nexus" between the alleged offenses and place to be searched. *See, e.g.*, *Griffith*, 867 F.3d at 1278 (good-faith exception inapplicable where warrant application alleged no factual nexus to home and improperly sought permission "to search for and seize any electronic device found in the home"); *United States v. Gonzales*, 399 F.3d 1225, 1231 (10th Cir. 2005) (exception inapplicable where affidavit alleged no facts showing even a "minimal nexus between the place to be searched and the suspected criminal activity;" detective merely stated that, in his general experience, "firearm[s] are often kept at the residence"); *United States v. McPhearson*, 469 F.3d 518, 527 (6th Cir. 2006) (exception inapplicable where "evidence in the affidavit connecting the crime to the residence is so vague as to be conclusory or meaningless").

Here, conclusory assertions aside, the affidavit provided no facts connecting Mr. Schulte's New York City apartment to the offenses, and no factual basis for assuming that any incriminating evidence would be found there in March 2017. Thus, *Leon's* good-faith exception does not apply. As the Supreme Court explained in *Leon*, the exception does not apply if a warrant is "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. at 923 (internal quotation marks omitted). When applying that standard, courts consider the objective reasonableness not only of "the officers who eventually executed the warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination." *Id.* at 923 n.24. The question is whether an objectively reasonable officer could believe in good faith that the affidavit established probable cause, keeping in mind the inadequacy of a "bare bones" affidavit. *Id.*

Though the March 13, 2017 warrant affidavit was lengthy, the allegations purporting to establish a nexus between the offenses and Mr. Schulte's apartment—contained in a single, conclusory paragraph of the affidavit—were "bare bones." *See United States v. Wilhelm*, 80 F.3d 116, 121 (4th Cir. 1996) (A "bare bones" affidavit is one that contains "wholly conclusory statements, which lack the facts and circumstances from which a magistrate can independently determine probable cause.") (quoting *United States v. Laury*, 985 F.2d 1293, 1311 n.23 (5th Cir. 1993)). Thus, they fell far short of permitting reasonable, good-faith reliance on the warrant.

The government's theory of probable cause to search the apartment ran as follows: (1) Mr. Schulte might have used a computer or another electronic device in March 2016 to copy and steal information belonging to the CIA; (2) if so, he might have kept such a device in his Virginia residence; (3) if so, he might have taken the device with him when he moved to New York City in November 2016; (4) if so, the computer or device might still be present in Mr. Schulte's New York City residence in March 2017; and (5) if so, the device might contain incriminating communications or other information about the theft of classified information allegedly committed a full year earlier.

Whatever may be the reasonableness of any one of these inferences standing on its own, demonstrating probable cause required adequately establishing all five in combination. The affidavit did not approach doing so. It provided no factual basis to believe Schulte even *had* a home computer or other electronic storage device when he lived in Virginia in 2016, much less that he used it to commit the offenses and brought it with him when he moved to New York. And with regard to whether any computer would retain any incriminating information about a CIA

infiltration occurring a full year beforehand, the affidavit observed only that computers, in general, can retain information for long periods. *See* 3/13/17 Aff. ¶ 27.

Additionally, the affidavit sought, and the warrant granted, authorization to seize and search every electronic storage device found in the home. When the FBI executed the warrant, they discovered a plethora of devices, requiring the FBI to apply for a new warrant the next day to seize the devices. The initial warrant's material overbreadth, discussed in more detail below, *see* Point IV, and the need to return to the magistrate for a second warrant, underscore the FBI's unawareness of the existence of any such devices in the first place (much less the existence of any having to do with the alleged offenses): given that law enforcement did not know whether Schulte even owned a computer or any other particular electronic device, they could not describe ex ante the specific devices they would search for and seize. But it was no solution to rely on a catchall provision authorizing the blunderbuss seizure and search of every device they might happen to find. Nothing in the affidavit supported—or constitutionally could have supported—a general warrant to seize and search any and all phones, tablets, computers, and other devices in the apartment.

Here, as explained, the affidavit failed to establish probable cause to believe that any computer (or other electronic device) containing incriminating information about the Classified Information Offenses would be found in Mr. Schulte's apartment in March 2017. Taken together, these failings as to probable cause and overbreadth bring the warrant beyond the good-faith exception's reach. *See Griffith*, 867 F.3d at 1278 (affidavit "fell short to an extent precluding good-faith reliance on the warrant"); *see also United States v. Leary*, 846 F.2d 592, 606–10 (10th Cir. 1988) (declining to apply the good-faith exception where warrant swept too broadly in describing the items subject to seizure and search).

Moreover, this conclusion does not require this Court to find bad faith on the part of law enforcement. The Supreme Court has found *Leon's* objective standard unmet even absent any reason to suppose that officers acted in bad faith in relying on an invalid warrant. *See Groh v. Ramirez*, 540 U.S. 551, 563-65 & n.8.

In sum, because the warrant affidavit failed to establish even a minimal factual connection between the alleged offenses and Mr. Schulte's residence, the warrant is invalid, the good-faith exception to the exclusionary rule is not applicable, and the Court should suppress the resulting evidence.

Point III

The warrants to search for evidence of child pornography are void because the FBI obtained them by deliberately or recklessly omitting material facts. Accordingly, the Court should suppress the resulting evidence. At a minimum, an evidentiary hearing is required.

The initial March 13, 2017 warrant application was not the only one in this case that was materially misleading. On April 14, 2017, and again on May 10, 2017, the FBI sought additional warrants to search Mr. Schulte's devices for evidence that he violated federal law by knowingly possessing or receiving child pornography. Each warrant application claimed that, while searching for evidence relating to the Classified Information Offenses, the FBI had found what "appear[ed] to be" an image of child pornography on Mr. Schulte's "desktop computer." But the applications deliberately or recklessly omitted key facts necessary to avoid misleading the magistrate: the image was found in a discrete, inaccessible area of the computer known as the "page file," the image contained no indicia to show when, if ever, it had last been opened or viewed, and it was partially blacked out. Had the FBI disclosed these facts, no probable cause would have existed to believe that Mr. Schulte had committed any pornography offense or

possessed other images of child pornography. Accordingly, the warrants are invalid under *Franks*, the good-faith exception does not apply, and suppression is required.

A. The FBI misled the magistrate by stating that the image was found on Mr. Schulte's "desktop computer," without disclosing that it was found in the "page file," had no meaningful data associated with it, and was partially blacked out.

The FBI's warrant applications presented a thin but seemingly straightforward case for probable cause to search Mr. Schulte's computers for evidence of child pornography. They claimed that the FBI had found a "photograph" of what "appear[ed]" to be child pornography on Mr. Schulte's "desktop computer." 4/14/17 Aff. ¶ 13; 5/10/17 Aff. ¶ 13.

This statement was literally true in the sense that the "photograph" or image was discovered on Mr. Schulte's "desktop computer," as opposed to a laptop computer. But even literally true statements violate *Franks* where the affiant has "intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading." *Liston v. Cnty. of Riverside*, 120 F.3d 965, 973 (9th Cir. 1997) (citation and internal quotations omitted); *see also United States v. Tate*, 524 F.3d 449, 456–57 (4th Cir. 2008) ("When an omission is involved, the question is not whether the affidavit was 'literally true,' but whether [defendant's] offer of proof made a showing that the warrant affidavit omitted facts by design to mislead the issuing judge … A 'literally true' affidavit thus can be intentionally misleading if it deliberately omitted material facts which, when included, would defeat the probable cause showing") (original emphasis deleted).

Here, the FBI misled the magistrate by stating that the alleged pornographic image was discovered on the "desktop computer," without disclosing where specifically it was found. As the FBI knew, the image was found in a special area of the computer known as the "page file." As explained in the accompanying declaration of computer scientist Steven M. Bellovin, Ph.D.,

the "page file" is an area of the computer that is generally inaccessible to a computer's users. *See* Bellovin Decl. ¶¶ 8–9. An image can be present in the page file even if no user of the computer ever saw it, knowingly accessed it, or intentionally acquired it. *Id.* ¶ 10. For example, if a person surfs the Internet for legal adult pornography, the computer's operating system can automatically "pre-fetch" (download) an image of child pornography that may be on a website—and it can wind up in a computer's page file without the user ever seeing the image. *Id*. The undisclosed fact that the image in this case was partially blacked out was consistent with such inadvertent acquisition. *See id.* ¶ 11.

The warrant affidavits further misled the magistrate by not disclosing that the image had virtually no "metadata" associated with it—meaning that the FBI did not know when the image had been created, acquired, or last viewed (if ever). *See* Bellovin Decl. ¶ 11. Thus, the image could have been present on the computer for years. *Id*. Disclosing this information to the magistrate would have shown that the scant evidence concerning the single image—which, incidentally, may not even qualify as child pornography because it does not appear to depict a real child—was too stale to justify a search of the computer in April and May of 2017. *See, e.g.*, *Walczyk v. Rio*, 496 F.3d 139, 162 (2d Cir. 2007) ("In evaluating probable cause, a magistrate is always required to consider whether the facts adduced in the warrant application 'appear[] to be current, i.e., true at the time of the application,' or whether they have 'become stale.' … Thus, where information is seven years old, a magistrate must be alerted to that fact to make a reasonable probable cause determination.").

B. The FBI omitted the information deliberately or with reckless disregard for the truth.

The FBI's decision to keep this important information about the lone "CP" image from the magistrate was a reckless, if not intentional, effort to mislead.

First, when the FBI first applied for the initial child pornography warrant, it already knew (or recklessly disregarded) that the image was found in the page file. The government's own documents indicate that the image was discovered in "pagefile.sys," unmistakable evidence that it was found in the page file. *See* Bellovin Decl. ¶ 7; Shroff Decl. Exh. H. But the FBI kept that important fact from the magistrate, supporting an inference of reckless or purposeful deception. *See, e.g., United States v. Castellanos*, 820 F. Supp. 80, 84 (S.D.N.Y. 1993) (Sotomayor, J.) ("Reckless disregard for the truth means failure to heed or pay attention to facts as [the affiant] knew them to be.") (citation and internal quotations omitted).

Further, FBI agents are presumed to know the law governing their conduct. *See, e.g.*, *Harlow v. Fitzgerald*, 457 U.S. 800, 819 (1982) ("a reasonably competent public official should know the law governing his conduct"). The Second Circuit has made clear for years that evidence that a person may have an interest in child pornography, or even may have accessed pornography online at some point, is not sufficient to establish probable cause to search his computer. *See, e.g.*, *Raymonda*, 780 F.3d at 117–18. Rather, the government must provide evidence that the person is likely a "collector" or "hoarder" of child pornography; absent such evidence, no basis exists to believe that the person currently possesses child pornography. *See id.* at 115, 117.

Thus, the FBI here was at least reckless in not disclosing that the image was discovered in the page file. As the FBI must have known, disclosing that fact would have undercut the existence of probable cause to believe that Mr. Schulte had ever viewed or knowingly accessed

the image—let alone "accessed [it] in circumstances sufficiently deliberate or willful to suggest that he was an intentional 'collector' of child pornography, likely to hoard [other] images." *Raymonda*, 780 F.3d at 117.

C. The misleading omissions were material to the probable cause determination.

The FBI's failure to disclose that the purported pornographic image was undated, found in the page file, and partially blacked out, was material because, if those facts been included in the warrant affidavit, probable cause would have vanished.

United States v. Raymonda is illustrative. There, the evidence showed that the defendant had used the Internet to access 76 "thumbnail images," the majority of which were images of child pornography, on a single occasion nine months before the government applied for a search warrant. 780 F.3d at 109–10. Further, expert testimony showed that the IP logs containing the thumbnail images "did not disclose whether" the user "had saved or even viewed all of the images that his browser had accessed, and indeed would have looked exactly the same even if he simply closed the site immediately after clicking on it." *Id.* at 111–12 (internal quotations marks and alteration omitted). The Circuit held that this evidence failed to establish probable cause for the search: "[A] single incident of access to thumbnail images of child pornography, absent any other circumstances suggesting that the suspect accessed those images deliberately or has a continuing interest in child pornography, fails to establish probable cause that the suspect will possess illicit images many months later." *Id*. at 109. Moreover, "[w]here the only evidence supporting a search warrant is equally consistent with a suspect's innocent stumble on an illicit website as with his deliberate access to child pornography, such evidence does not support an inference that the suspect is a 'collector' likely to hoard pornographic images past the time that his computer would overwrite the images in the ordinary course." *Id*. at 121.

The evidence against Mr. Schulte was even weaker than in *Raymonda*. The warrant application provided no evidence that Mr. Schulte had ever visited an illicit website or knowingly accessed any image of child pornography—even once—much less that he did so within nine months of the proposed search. In *Raymonda*, the Circuit relied on expert testimony concluding that the manner in which illicit images appeared on the defendant's IP logs provided no evidence that "the user subsequently saved the illicit thumbnails to his hard drive, or that he even saw all of the images, many of which may have downloaded in his browser outside immediate view." *Id.* at 117. Similarly, as Professor Bellovin's declaration explains, because of the unique attributes of a page file, the discovery of the single alleged pornographic image in the page file did not "provide a basis for concluding that the …image was ever seen, intentionally accessed, or knowingly possessed" by Mr. Schulte. Bellovin Decl. ¶ 10. For that reason, the FBI's discovery of the lone image was at least "equally consistent with [Mr. Schulte's] innocent stumble on an illicit website as with his deliberate access to child pornography." *Raymonda*, 780 F.3d at 121. And the search warrant affidavit offered no other evidence that Mr. Schulte was likely to be a "collector" or "hoarder" of illegal pornographic material. Accordingly, under *Raymonda*, once the misleading omissions are corrected, the already thin evidence of probable cause vanishes altogether. That makes the misleading omissions "material." *Id.*; *see also United States v. Falso*, 544 F.3d at 120–21 (no probable cause existed where warrant application alleged only that defendant "appeared" to have accessed or attempted to access a website that contained about 11 images of child pornography, and had an 18-year-old conviction for sexual abuse of a minor, without any allegation defendant had in fact accessed the website at issue).

To be sure, the April 10, 2017 warrant affidavit also claimed that Mr. Schulte had "apparently" searched, five or six years earlier, in 2011 and 2012, for "child pornography" on

Google. But those old Google searches were found during an illegal FBI search for child pornography that exceeded the scope of the Online Account Warrants. *See* 5/10/17 Aff. ¶ 14 n. 6 (conceding that the FBI had searched for evidence of child pornography before obtaining a warrant to do so). Accordingly, the Court may not consider those Google searches in assessing whether the affidavit would have established probable cause even without the misleading description of the found image. *See, e.g., United States v. Trzaska*, 111 F.3d 1019, 1026 (2d Cir. 1997) ("'[A] reviewing court should excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant.'").

In summary, Mr. Schulte has made at least a "substantial preliminary showing" under *Franks* that the child pornography warrants intentionally or recklessly omitted important facts in an effort to mislead, and that those omissions were material to the probable cause determination. Accordingly, the Court should conduct a *Franks* hearing, declare the warrants void, and suppress the resulting evidence.

Point IV

The warrants allowing a search of virtually everything in Mr. Schulte's home, all of his electronic data, and all of the information associated with his online accounts were overbroad and insufficiently particularized.

A. The Fourth Amendment prohibits general warrants.

As noted earlier, the Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." "The Fourth Amendment's requirements regarding search warrants are not 'formalities.'" *United States v. Voustianiouk*, 685 F.3d 206, 210 (2d Cir. 2012) (quoting *McDonald v. United States*, 335 U.S. 451, 455 (1948)). "The chief

evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" *Galpin*, 720 F.3d at 445 (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)). "To prevent such 'general, exploratory rummaging in a person's belongings' and the attendant privacy violations, the Fourth Amendment provides that a 'warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity.'" *Id*. (internal citations omitted) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

The particularity requirement has three components. "First, a warrant must identify the specific offense for which the police have established probable cause. Second, a warrant must describe the place to be searched. Third, the warrant must specify the items to be seized by their relation to designated crimes." *Galpin*, 720 F.3d at 445–46 (internal citations omitted). In addition, "courts in this Circuit have identified certain 'circumstance-specific considerations' that may bear on whether a given warrant lacks particularity, even if they do not constitute formal, universal requirements." *United States v. Wey*, 256 F. Supp. 3d 355, 381 (S.D.N.Y. 2017) (quoting *United States v. Zemylansky*, 945 F. Supp. 2d 438, 454 (S.D.N.Y. 2013)). "Many courts, for example, "'have found warrants for the seizure of ... records constitutionally deficient where they imposed too wide a time frame or failed to include one altogether.'" *Id*. (quoting *Zemylansky*, 945 F. Supp. 2d at 454, and collecting cases). In addition to ensuring that there is probable cause to seize and search, courts must also give special attention to whether a warrant is impermissibly overbroad. A search warrant is overbroad in violation of the Fourth Amendment if its "description of the objects to be seized is ... broader than can be justified by the probable cause upon which the warrant is based." *Galpin*, 720 F.3d at 446. A warrant that purports to

"authorize the seizure of, essentially, all documents" exceeds the scope of probable cause. *Wey*, 256 F. Supp. 3d at 393.

These principles apply with special vigor to searches of digital devices—especially those kept in the home. "Where ... the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance." *Galpin*, 720 F.3d at 446. That is because the "seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure." *United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2016) (en banc). As such, "[t]he potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous"—a "threat [that] is compounded by the nature of digital storage." *Galpin*, 720 F.3d at 447.

Suppression is appropriate where the search warrant affidavit is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at923 (internal quotation marks omitted).

B. The warrants here were general, overbroad warrants that lacked particularity.

The many warrants in this case allowed the government to seize and search Mr. Schulte's property, all of his electronic devices (including 12 terabytes of electronic data), and all of the information associated with his Google, Reddit, and GitHub accounts. These were general warrants that lacked the specificity required for any kind of tailored search. For example, the initial March 13, 2017 warrant laid out several broad categories of information sought by law

enforcement. While this enumeration may appear to have limited the scope of the warrant, in reality it comprehensively listed all of the data that can be stored on an electronic device.

The particularity requirement "is necessarily tied to the … probable cause requirement." *In re 650 Fifth Ave. & Related Props.*, 830 F.3d 66, 99 (2d Cir. 2016). "'By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.'" *Id*. (quoting *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

The warrants here authorized the government to seize and search virtually everything they could find relating to Mr. Schulte. The warrants authorized the search and seizure of a litany of information, "including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes," as well as of any electronic devices and storage media that contained such information. *E.g.*, 3/13/17 Aff., Attach. A, III.A, ¶¶ 3–4. They further authorized search and seizure of "[a]ny evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media." *Id.*, Attach. A, III.B. True, many of the categories of sought information came with qualifying language. *E.g., id.,* Attach. A, III.A, ¶ 5 (evidence of the user's state of mind "as it relates to the Subject Offenses"). But this language did no limiting work: an agent reviewing Mr. Schulte's electronic information could not know whether or not it "relate[d] to the Subject Offenses" without reading it, as even the government acknowledged: "[L]aw enforcement may use various techniques" to review the electronic data "for information responsive to the warrant." Such techniques included "opening or cursorily reading the first few 'pages' of such files in order to determine their precise contents." *Id.*, Attach. A, III.C.

Moreover, several of these categories—most notably, "[a]ny evidence concerning the persons with access to … the seized" electronics, *id.*, Attach. A, III.B, but also all of the items listed in Subsection B—had no limitations at all. These were impermissibly overbroad because they described generic types of data without any reference to the suspected criminal conduct. *See Wey*, 256 F. Supp. 3d at 385 (warrant lacked particularity where it set forth "expansive categories of often generic items subject to seizure—several of a 'catch-all' variety—without, crucially, any linkage to the suspected criminal activity"). Those defects appeared here, as these warrants purported to authorize searches for any evidence concerning "the persons with access to" Mr. Schulte's computer—including, inevitably, Mr. Schulte himself—without specifying to whom or to what that evidence might relate. *See* 3/13/17 Aff., Attach. A, III.B.

The warrants also lacked any temporal limitation on the files for which the government could search. Because the warrants described alleged criminal activity beginning in March 2016, it would have been appropriate (and feasible) to limit any search to records relating to that time period and afterwards. Instead, the warrants authorized a nearly boundless search of personal data across several devices. For example, each of the Online Account Warrants set forth a series of categories of essentially unlimited information, including 14 categories for Google, 7 categories for Reddit, and 9 categories for GitHub. The companies were inexplicably directed to turn over materials dating back to Mr. Schulte's first use of the accounts, which in the case of Google was *11 years'* worth of information. Such an open-ended intrusion was unsupported by probable cause, facially overbroad, and devoid of the particularity demanded by the Fourth Amendment. *See, e.g.*, *Wey*, 256 F. Supp. 3d at 387 (warrant lacked particularity for failing to include a date range, despite "rather precise timeframes" identified in an unincorporated affidavit); *United States v. Levy*, 2013 WL 664712, at *11 n.7 (S.D.N.Y. Feb. 25, 2013)

("Several courts in this Circuit have recognized the constitutional questions that are raised by the lack of a specific date range in a warrant for documentary records and warned the Government to include one when possible.") (citing cases), *aff'd*, 803 F.3d 120 (2d Cir. 2015). Altogether, the warrants to search Mr. Schulte's electronic data "lacked the requisite specificity to allow for a tailored search of [the defendant's] electronic media" and "fail[ed] to link the items to be searched and seized to the suspected criminal activity." *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010).

The Second Circuit has noted that digital searches "demand[] a heightened sensitivity to the particularity requirement" because of the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Galpin*, 720 F.3d at 447 (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (quotation marks omitted)). But general warrants are precisely what the government sought and obtained in this case. Accordingly, those warrants violate the Fourth Amendment, necessitating suppression of the resulting evidence**.**

CONCLUSION

For these reasons, this Court should hold an evidentiary hearing under *Franks*, grant suppression, and direct any other relief that may be appropriate.

Dated: New York, New York
July 3, 2019

Respectfully submitted,

Federal Defenders of New York, Inc.

/s/
Sabrina P. Shroff

Sabrina P. Shroff
Edward S. Zas
Allegra Glashausser
Assistant Federal Defenders
52 Duane Street, 10th Floor
New York, New York 10007
Tel.: (212) 417-8713

Counsel for Defendant Joshua Adam Schulte