

**Federal Defenders
OF NEW YORK, INC.**

Southern District
52 Duane Street-10th Floor, New York, NY 10007
Tel: (212) 417-8700 Fax: (212) 571-0392

David E. Patton
Executive Director

Southern District of New York
Jennifer L. Brown
Attorney-in-Charge

February 18, 2020

Hon. Paul A. Crotty
United States District Judge
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: *United States v. Schulte*, S2 17 Cr. 548 (PAC)

Dear Judge Crotty:

Defendant Joshua Adam Schulte respectfully moves for a mistrial because the government has improperly withheld critical discovery and trial materials, including exculpatory information, in violation of the Fifth and Sixth Amendments and the Federal Rules of Criminal Procedure.

First, the government failed to disclose an internal August 2019 memorandum from the Deputy Director of the CIA for Counterintelligence to the Director of Security requesting that one of its employees, known to the jury as “Michael,” be placed on enforced administrative leave because of suspicion, *inter alia*, that he was involved in the theft and disclosure of the Vault 7 and Vault 8 information (the “CIA Memorandum”). The request was granted and Michael has been on paid leave ever since. This information and any related documents should have been disclosed to the defense pursuant to *Brady v. Maryland* and Fed. R. Crim. P. 16 promptly in August 2019—not in the middle of Michael’s cross-examination six months later. *See* Tr. 1333.

Second, despite repeated requests, the government improperly refused to permit the defense to inspect or copy the “mirror images”¹ of the CIA’s ESXi Server and FS01 Server (also known as the “NetApp” Server) (collectively, the “CIA Servers”). Yet, as revealed by the government’s forensic expert Patrick Leedom

¹ “A ‘mirror image’ of a computer is an exact copy of the data contained in a particular digital storage unit, such as a computer hard drive. Computer code is a series of zeroes and ones, each of which is called a bit; making a mirror image is copying each zero or one in sequence, bit by bit.” *United States v. Ganius*, No. 08 Cr. 224 (AWT), 2011 WL 2532396, at *2 n.1 (D. Conn. Jun. 24, 2011).

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 2
February 18, 2020

during his testimony, the government permitted *him* to examine these mirror images all along—an examination that appeared essential to his testimony and conclusions. Moreover, the testimony of other government witnesses, including “Dave ” and FBI Agent Berger, could not be adequately tested by the defense because, unlike the government, we did not have access to the mirror images.

The government’s misconduct has severely prejudiced the defense. If the withheld information had been timely disclosed, it would have materially affected every aspect of the trial preparation and defense, including counsel’s overall strategy. The improperly withheld information would have substantially strengthened the defense’s ability to cross-examine the government’s witnesses, and buttressed the defense’s argument that someone other than Mr. Schulte copied and disclosed the Vault 7 and Vault 8 information. At this point in the trial, this prejudice cannot be remedied merely by granting a continuance, striking or re-opening testimony, or issuing curative instructions. A mistrial is necessary.

FACTS

The Failure to Disclose the CIA Memorandum

In the middle of trial, on the evening of February 11, 2020—the day before Michael’s direct examination—the government notified the defense for the first time that the CIA had placed him administrative leave in August 2019. When defense counsel asked why, the government advised that the CIA was not satisfied with Michael’s cooperation during the investigation into the Vault 7 and Vault 8 leaks.

The next morning, defense counsel asked the Court to direct the government to turn over to the defense, or to review *in camera*, any CIA document explaining its decision to place Michael on leave. The government opposed this request, arguing that defense counsel already had everything she needed to cross-examine Michael. The Court ordered the government to produce the documents that evening for *in camera* review.

The following morning, while Michael’s cross-examination was still underway, the Court directed the government to give defense counsel the document it had reviewed *in camera*. The document—a five-page memorandum from the Deputy Director to CIA security officials—was a bombshell. It showed, among other things, that the CIA itself had determined that Michael was a credible suspect in the theft. It said that “[s]everal concerns about [Michael] have emerged” in the CIA’s review of his investigation, “including his proximity to the theft of the data. The CIA found that Michael a) may have information regarding the theft that he is withholding; b) has failed to clear himself after routine questioning as well as questioning under polygraph; and, c) shows “a lack of concern” about the loss that the CIA suffered as a result of the leak. The memorandum found that Michael was

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 3
February 18, 2020

a security risk, recommended immediate deactivation of Michael's badge, and advised that he be placed on administrative leave. CIA Memorandum at 3.

Following an *in camera* and *ex parte* conference with defense counsel, the Court granted the defense's motion to suspend Michael's examination indefinitely. It admonished the government for failing to produce the CIA Memorandum to the defense in August 2019. As the Court stated, "the basis [for suspending the examination] is the late production of this information. I believe it should have been turned over at or about the time that the decision was made. And I think it was not accurate and not correct for you to withhold that information until the witness took the stand." Tr. 1334.

The Failure to Provide the Defense Access to the Mirror Images of the CIA Servers

As the trial testimony thus far demonstrates, this prosecution is a forensic "whodunit"—a circumstantial case involving complex, highly technical computer information regarding which individuals had the means, motive, and opportunity to access and transmit certain information at various points in time.

Since at least September 2018, the defense has asked the government over and over again to provide the mirror images of the CIA Servers—the forensic crime scene. The government has consistently refused to do so, persuading the Court—in *ex parte* CIPA submissions—that the defense was not entitled to these images because they were not "material" and contained classified information that was too sensitive even for cleared defense counsel to see. Instead of producing the mirror images, the government provided only select "forensic cases" obtained from the CIA Servers—essentially, a subset of only those computer files the government deemed relevant and discoverable. The defense wrote to the Court numerous times in an effort to obtain the full mirror images, to no avail.

Then, in the midst of trial, Mr. Leedom, the government's retained forensic computer expert, testified that *he* had been granted full and unrestricted access to the mirror images of the CIA Servers and other CIA computers. That access enabled Leedom to perform numerous tests and analyses that the defense has not been able to replicate or refute. He characterized access to these mirror images as essential to his expert testimony. Specifically, Mr. Leedom testified on cross-examination that he and his team "were given images of all DevLAN machines—computers, servers—that were available at the time that we showed up to analyze," that he had access to "mirror images of almost every network and computer that [he] needed from the CIA," and that these mirror images "very much informed [his] expert testimony" at the trial. Tr. 1159, 1187.

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 4
February 18, 2020

ARGUMENT

This Court has “broad discretion” to grant a mistrial. *Renico v. Lett*, 559 U.S. 766, 774 (2010). A mistrial is appropriate whenever, taking all the circumstances into consideration, there is a “manifest necessity” for the act. *Id.*

Here, a mistrial is required for two separate but equally compelling reasons. First, the government improperly withheld *Brady* information from the defense (the CIA Memorandum) until the Court, upon *in camera* review, ordered disclosure on February 13, 2020. Second, the government denied the defense and its expert any access to the mirror images of the CIA Servers—access the defense *still* does not have—while granting unfettered access to its own testifying expert. The withholding of this information violated Rule 16 and the Constitution, was fundamentally unfair to the defense, and is highly prejudicial. Thus, the government has left this Court with no choice but to grant a mistrial.

I. The government’s failure to disclose the CIA Memorandum until the middle of Michael’s cross-examination requires a mistrial.

A. The Fifth and Sixth Amendments required the government to disclose the CIA Memorandum because it contains information favorable to the defense.

Under *Brady v. Maryland*, 373 U.S. 83 (1963), the Fifth Amendment requires the government to disclose evidence that is favorable to the defense. “There are three components of a true *Brady* violation: The evidence at issue must be favorable to the accused, either because it is exculpatory, or because it is impeaching; that evidence must have been suppressed by the State, either willfully or inadvertently; and prejudice must have ensued.” *United States v. Rivas*, 377 F.3d 195, 199 (2d Cir. 2004) (quoting *Strickler v. Greene*, 527 U.S. 263, 281–82 (1999)).

All three components exist here. First, the CIA Memorandum is both exculpatory and impeaching. It is exculpatory because it suggests that “Michael” was involved in the leak of the materials Mr. Schulte is charged with leaking and, therefore, that he is an alternative perpetrator. This is “classic *Brady* material.” See *Boyette v. Lefevre*, 246 F.3d 76, 91 (2d Cir. 2001) (explaining that information that “could have helped the defense suggest an alternative perpetrator” was “classic *Brady* material”); see also *Mendez v. Artuz*, 303 F.3d 411, 413 (2d Cir. 2002) (evidence that “supplies a possible alternate perpetrator” is *Brady* material). The Second Circuit has squarely held that “specific, concrete evidence” that someone other than the defendant committed the crime is “without question ... of a nature requiring pretrial disclosure to allow for full exploration and exploitation by the defense.” *Leka v. Portuondo*, 257 F.3d 89, 101 (2d Cir. 2001) (quoting *Grant v. Alldredge*, 498 F.2d 376, 382 (2d Cir. 1974)). The CIA Memorandum is also

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 5
February 18, 2020

impeaching because it suggests that, according to the CIA itself, Michael has not been truthful in his many interactions with FBI and CIA investigators. And, by lying to the FBI, Michael may have committed serious federal crimes.

Second, the CIA Memorandum was suppressed. To establish that evidence was “suppressed,” the defendant need not show that the government acted intentionally or in bad faith. Indeed, the government’s state of mind is irrelevant. *See, e.g., Strickler*, 527 U.S. at 282 (affirming that *Brady* violation can be “inadvertent[]”); *see also United States v. Douglas*, 525 F.3d 225, 245 (2d Cir. 2008) (*Brady* material that is “not disclosed in sufficient time to afford the defense an opportunity for use may be deemed suppressed within the meaning of the *Brady* doctrine”).

Third, the suppression of the evidence was prejudicial. To show prejudice, the defendant must show materiality:

A showing of materiality does not require demonstration by a preponderance that disclosure of the suppressed evidence would have resulted ultimately in the defendant’s acquittal The touchstone of materiality is a reasonable probability of a different result, and the adjective is important. The question is not whether the defendant would more likely than not have received a different verdict with the evidence, but whether in its absence he received a fair trial, understood as a trial resulting in a verdict worthy of confidence.

Leka, 257 F.3d at 104 (quoting *Kyles v. Whitley*, 514 U.S. 419, 434 (1995)). “While *Brady* ensures a fair trial, a defendant’s right to pre-trial disclosure under *Brady* is not conditioned on his ability to demonstrate that he would or even probably would prevail at trial if the evidence were disclosed,” much less that he is in fact innocent. *Poventud v. City of New York*, 750 F.3d 121, 133 (2d Cir. 2014) (quoting *Osborne v. Dist. Att’y’s Office for Third Jud. Dist.*, 521 F.3d 1118, 1132 (9th Cir. 2008), *rev’d on other grounds*, 557 U.S. 52 (2009)). “The remedy for a *Brady* claim is therefore a new trial, as proof of the constitutional violation need not be at odds with his guilt.” *Id.* (citing *United States v. Sipe*, 388 F.3d 471, 493 (5th Cir. 2004)).

The prejudice to Mr. Schulte is apparent. A criminal defendant has a constitutional right at trial to present evidence tending to prove that someone else may have committed the crime with which he is charged. *See, e.g., United States v. White*, 692 F.3d 235, 245–46 (2d Cir. 2012). Though the government turned over some evidence in discovery (mainly 302’s) suggesting that Michael may have behaved suspiciously by taking a “screenshot” of the computer reversion on April 20, 2016, and may later have been untruthful with the FBI, the CIA Memorandum revealed for the first time that the CIA *itself*, after an exhaustive investigation, had determined that Michael was (and remains) a legitimate suspect in the crime. And

Hon. Paul A. Crotty
 Judge, Southern District of New York

Page 6
 February 18, 2020

the CIA Memorandum disclosed other new information as well: Michael was placed on “enforced administrative leave” in August 2019, was too great a security threat to remain working inside the CIA’s offices, and had failed to clear himself after two polygraph examinations, among other revelations. This is critical information that could have been used to bolster Mr. Schulte’s defense at trial and to suggest that someone else may have been responsible for the crimes with which he is charged. Moreover, one of the major strategic trial decisions for the defense was whether, and how aggressively, to blame Michael for the theft and disclosure of the Vault 7 and Vault 8 information. This CIA Memorandum would have been critical to informing that decision. It was obviously improper under *Brady* for the government to fail to disclose this information in time for it to be used effectively by the defense in this trial, and the government’s actions require a mistrial.

B. The government’s belated, mid-trial disclosure of the CIA Memorandum also violates Rule 16.

Rule 16 of the Federal Rules of Criminal Procedure requires the government to grant a defendant access to documents, data, and other information within the “government’s possession, custody, or control” if the items are “material” to preparing the defense, or the government intends to use the items in its case-in-chief at trial. *See* Fed. R. Crim. P. 16(a)(1)(E)(i)-(ii); *see also United States v. Rigas*, 258 F. Supp. 2d 299, 306 (S.D.N.Y. 2003). The Rule further provides that, if a party fails to comply with its discovery obligations under the rule, the court may grant a continuance, prohibit that party from introducing the undisclosed evidence, or enter any other order that is just under the circumstances. Fed. R. Crim. P. 16(d)(2). “When the government has failed to comply with Rule 16, the district court has broad discretion to determine what remedial action, if any, is appropriate.” *United States v. Miller*, 116 F.3d 641, 681 (2d Cir. 1997).

The “materiality standard of Rule 16 normally is not a heavy burden.” *United States v. Stein*, 488 F. Supp. 2d 350, 356 (S.D.N.Y. 2007) (quoting *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993)). *See also* 2 Charles Alan Wright *et al.*, *Federal Practice and Procedure—Criminal* § 254 (4th ed. 2013) (“Too much should not be required in showing materiality.”). An item is “material” if “it could be used to counter the government’s case or to bolster a defense.” *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993) (internal citations omitted). In other words, evidence is “material” if its pretrial disclosure will enable a defendant to alter significantly the quantum of proof in his favor. *United States v. McGuinness*, 764 F. Supp. 888, 895 (S.D.N.Y. 1991); *accord United States v. Maniktala*, 934 F.2d 25, 29 (2d Cir. 1991); *United States v. Giffen*, 379 F. Supp. 2d 337, 342 (S.D.N.Y. 2004).

Rule 16 is not confined to documents within the prosecutors’ possession or direct control. *See Kyles*, 514 U.S. at 437 (“prosecutor has a duty to learn of any

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 7
February 18, 2020

favorable evidence known to the others acting on the government's behalf in the case, including the police"). Rather, Rule 16 is an "anti-withholding provision." *United States v. Trevino*, 556 F.2d 1265, 1272 (5th Cir. 1977). A prosecutor is not "allowed to avoid disclosure of evidence by the simple expedient of leaving relevant evidence to repose in the hands of another agency while utilizing his access to it in preparing his case for trial." *Trevino*, 556 F.2d at 1272; *see also United States v. Bryan*, 868 F.2d 1032, 1035–36 (9th Cir. 1989) (scope of Rule 16 obligation turns on "the extent to which prosecutor has knowledge of and access to the documents sought by the defendant in each case").

Material documents that the prosecution has reviewed or has access to must be provided to aid a defendant in preparing his defense. *See, e.g., United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995) (extending Rule 16 obligation to documents possessed by Bureau of Prisons, where prosecutors "had knowledge of and access to" documents); *United States v. Zuno-Arce*, 44 F.3d 1420, 1427 (9th Cir. 1995) (prosecutor is "deemed to have knowledge of and access to anything in the custody or control of any federal agency participating in the same investigation of the defendant"); *Trevino*, 556 F.2d at 1272 (noting that evidence accessible to the prosecution must be turned over to defendant, even if evidence is not within prosecution's "physical possession"); *United States v. NYNEX Corp.*, 781 F. Supp. 19, 25 (D.D.C. 1991) (holding that prosecution must produce materials possessed by other federal agencies allied with the prosecution).

For the reasons described above, there can be no question that the CIA Memorandum is "material" to the defense and within the government's possession or control. The document states that Michael worked in EDG until the summer of 2016, was a "software exploit developer with highly sensitive access", and was a system administrator for the DevLAN network. CIA Memorandum at 2. It states that Michael's security processing was paused in the wake of the WikiLeaks releases because of his system administrator access on DevLAN, "the system from which the tool was stolen." And the document was in the government's possession, custody, or control because the prosecutors, the FBI, and the CIA have been working in concert throughout this case. Accordingly, as the Court has already recognized, the government should have produced the CIA Memorandum to the defense months ago. In addition to violating the prosecutors' *Brady* obligations, withholding this document also violated Rule 16, to Mr. Schulte's great detriment.

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 8
February 18, 2020

II. The government's failure to permit the defense to inspect or copy the mirror images of the CIA Servers, while allowing the government's own expert to do so, requires a mistrial.

A. Rule 16 required the government to permit the defense expert to examine the mirror images of the CIA Servers.

Rule 16 also required the government to grant the defense access to the mirror images of the CIA Servers. *See, e.g., United States v. Hill*, 322 F. Supp. 2d 1081, 1091 (C.D. Cal. 2004) (holding that Rule 16 material can include “mirror image” copies of computer evidence). The Second Circuit has recognized that “[r]etention of the original storage medium or its mirror may ... be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved.” *United States v. Ganas*, 824 F.3d 199, 215 (2d Cir. 2016) (en banc) (citing, *e.g., United States v. Kimoto*, 588 F.3d 464, 480 (7th Cir. 2009) (quoting the defendant’s motion as stating: “Upon beginning their work, [digital analysis experts] advised [the defendant’s] Counsel that the discovery provided to the defense did not appear to be a complete forensic copy, and that such was necessary to verify the data as accurate and unaltered.”)). “Defendants may also require access to a forensic copy to conduct an independent analysis of precisely what the government’s forensic expert did—potentially altering evidence in a manner material to the case—or to locate exculpatory evidence that the government missed.” *Ganas*, 824 F.3d at 215. *See also Kimoto*, 588 F.3d at 480–81 (“[The defendant] argued that the failure to provide him with a complete forensic copy of all digital files impaired his ability to prepare a defense.”); Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 41 (2015) (“The forensic examiner ... generate[s] reports, detailing the protocols and processes that he or she followed.... The forensic reports must provide enough data to allow an independent third-party examiner to recreate the exact environment that yielded the report’s findings and observations.”); Darren R. Hayes, *A Practical Guide to Computer Forensics Investigations* 116 (2015) (“[B]ecause forensics is a science, the process by which the evidence was acquired must be repeatable, with the same results.”).

Courts have made clear that all material information available on electronic storage media is discoverable, whether readily readable (“active”) or “deleted” but recoverable. *See, e.g., Santiago v. Miles*, 121 F.R.D. 636, 640 (W.D.N.Y. 1988) (a request for “raw information in computer banks” was proper and obtainable under the discovery rules); *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 167 F.R.D. 90, 112 (D. Colo. 1996) (making mirror-image copy of everything on a hard drive was “the method which would yield the most complete and accurate results”; court chastises party’s expert for failing to do so).

Hon. Paul A. Crotty
 Judge, Southern District of New York

Page 9
 February 18, 2020

Here, the mirror images of the CIA Servers were clearly material to the defense—just as they were material to the government’s expert. While the government convinced the Court that these images could not be disclosed to the defense without jeopardizing the national security of the United States, the government had no trouble providing the images to the private expert it had retained. This unfairness violates both the letter and spirit of Rule 16 and CIPA.

B. The Fifth and Sixth Amendments required the government to permit the defense expert to examine the mirror images of the CIA Servers, just as the government’s expert was allowed to do.

By granting its own forensic expert full access to the mirror images of the CIA Servers, but denying the defense expert any access to them, the government has also denied Mr. Schulte his constitutional rights to due process, confrontation, compulsory process, effective assistance of counsel, and to present a complete defense. As the Supreme Court has held, rules about pretrial discovery in criminal prosecutions must apply to prosecutors as well as to defendants. *See Wardius v. Oregon*, 412 U.S. 470 (1973). This means that “[a]ccess [to mirror images] provided to private experts retained by the prosecution must be provided to private experts retained by the defense.” *United States v. Shrake*, 515 F.3d 743, 747 (7th Cir. 2008); *see also id.* (defense counsel had the right to “access on equal terms” to mirror image made available to prosecution’s expert).

Here, the government not only failed to provide “access on equal terms,” *id.*, it denied Mr. Schulte *any* access to the mirror images of the CIA Servers, claiming that such images were neither “material” nor “helpful” to the defense. Yet, at the very same time, it gave its expert *full* access to those images. This lopsided differential in access to crucial evidence was improper, fundamentally unfair, and, as we now show, highly prejudicial.

C. The prejudice resulting from the government’s conduct requires a mistrial.

The government’s failure to produce the mirror images has severely undermined the defense’s ability to represent Mr. Schulte. Here are ten specific (and non-exhaustive) examples of prejudice the defense has already suffered (and, of course, the trial is not yet over):

1. *The defense could not do the same analysis the government could do regarding alleged damage to the March 3, 2016 Confluence backup file.* Mr. Leedom testified at length regarding the crucial March 3, 2016 Confluence backup file that Mr. Schulte allegedly accessed via the NetApp Server on April 20, 2016. Leedom testified that this file was damaged in certain respects and that this damage enabled him to rule out certain theories about how the Vault 7 and Vault 8

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 10
February 18, 2020

information was acquired and leaked. *See* Tr. 1116–19. The defense, however, has never had access to the mirror image of the NetApp Server. As a result, the defense was (and remains) unable to examine the damage to the March 3 file and thereby test the reliability of Leedom’s analysis.

2. The defense could not analyze “vi-client logs” the way the government could. Mr. Leedom testified about “vi-client logs” recovered from Mr. Schulte’s CIA workstation. *See, e.g.*, Tr. 984–86, 1058–66, 1083–87. Such logs show things like virtual machine reversions. The defense, however, could not examine vi-client logs from anybody else’s workstations at the CIA, including Michael’s. These logs would have enabled the defense to determine whether any other employees conducted computer reversions or engaged in other suspicious activity relating to the theft of the Vault 7 and Vault 8 information.

3. The defense could not refute “Dave ’s” testimony about placing special restrictions on his home directory. Dave testified that he protected his home directory with special restrictions so that other people would not be able to access the information on it—including a copy of the Stash backup file. *See* Tr. 787-778, 795-96. The government had the ability to verify Dave ’s testimony, but presented no technical evidence to support it, despite presenting analogous technical evidence—the “last access” time to Rufus’s SSH key—when it supported their argument. *See* Tr. 867. The defense, in contrast, had no ability to examine the mirror image of the NetApp Server to see if Dave ’s testimony was accurate and, if not, to impeach him on cross-examination. The government did produce to the defense a screenshot of Dave ’s home directory, but this information provided the defense only with pictures of the directory, not the necessary technical information. The information did not allow the defense to check the permissions on his home directory to determine whether his testimony was accurate.

4. The defense was unable to determine which computers on the DevLan network were able to access the Altabackup files. Because the defense has never had access to the mirror image of the NetApp Server, the defense has been unable to examine the “NFS export list” for the Altabackup files. This list would have revealed which computer users on the DevLAN network could access the Altabackup files. Mr. Leedom, in contrast, *did* have this information and used it to the government’s advantage. While various 302’s indicate that the Altabackup files were not secure, Mr. Leedom used evidence that Mr. Schulte tried unsuccessfully to access the Altabackups (on April 15, 2016) to suggest that those files were not as vulnerable as the 302’s claimed. *See* Tr. 980–86. If the defense had been given access to the NetApp Server’s mirror image, it could have challenged Leedom’s conclusions.

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 11
February 18, 2020

5. *The defense could not adequately challenge government testimony relating to damage to the March 3, 2016 Confluence backup file.* When Mr. Branden was cross-examining Agent Berger, counsel asked whether the information published by WikiLeaks could have come from backup files created after March 3, 2016. Berger said that this was unlikely because of certain damage to the March 3 backup file. *See* Tr. 1413-1414. But the defense could not challenge this testimony because we were never given the mirror image of the NetApp Server, which would have allowed detailed analysis of the damaged file.

6. *The defense could not challenge Leedom's testimony concerning evidence found in "unallocated space."* Mr. Leedom testified regarding information he discovered in so-called "unallocated space" on the CIA's ESXi server. *See* Tr. 966-67, 1033. Because the defense was never provided the mirror image of the EXSi server, we had no access whatsoever to this unallocated space. *See Communications Center, Inc. v. Hewitt*, 2005 WL 3277983, at *1 (E.D. Cal. Apr. 5, 2005) (describing a "mirror image" as "a forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive") (emphasis added).I

7. *The defense was prevented from showing that there were other means to access the Altabackup files.* The defense cross-examined Dave about whether it was possible to obtain access to the Altabackup files via something called "CIFS." *See* Tr. 888-90. Without being provided the mirror image of the NetApp Server, the defense could not demonstrate that such access was indeed possible.

8. *The defense could not show how vulnerable the NetApp "DS00" file system was.* Because the defense was denied access to the NetApp mirror image, we could not evaluate or show the jury how insecure the DSOO file system was.

9. *The defense would have been able to determine access times to the Altabackup files without alerting the government to their significance.* Had the government granted the defense access to a mirror image of the NetApp server, the defense would have been able to determine on its own which files were accessed at which times. Instead, because the government denied us the mirror image, the defense had to specifically ask the government (in January 2020) to produce the access times for the Altabackups—a request that allowed the government to assert that the March 3, 2016 Confluence was accessed on April 20, 2016, during the Reversion Period. The defense should not have been placed in the position of having to focus the government on potentially incriminating evidence its own experts had not found.

10. *The defense would have been able to determine whether another user had root user access to the Confluence password page.* Given the belated, mid-trial disclosure regarding Michael, the defense should have been allowed to examine the

Hon. Paul A. Crotty
Judge, Southern District of New York

Page 12
February 18, 2020

Confluence VM to determine if he would have had access to files that Mr. Schulte is accused of stealing. Full access to the Confluence VM, which resided on the ESXi server, would have allowed the defense to investigate whether other CIA employees, including Michael, had access to the relevant data.

These examples are just a few of the many ways the defense has been seriously prejudiced by the government's failure to produce the mirror images of the CIA Servers. And these examples only scratch the surface: access to the mirror images could have allowed the defense to discover additional exculpatory, impeaching, or other helpful information—we still do not know because we still do not have access.

Dr. Steven Bellovin, the defense forensic expert, has informed us that, even if he were provided the mirror images of the CIA Servers now, he would need at least six months to replicate Mr. Leedom's analysis, examine the data thoroughly, and reach reliable conclusions. Under these circumstances, a mistrial is necessary.

CONCLUSION

For these reasons, the Court should grant a mistrial. Alternatively, the Court should grant the defense immediate access to the mirror images of the CIA Servers, order a lengthy trial continuance, strike or re-open the testimony of Mr. Leedom, "Dave," and Agent Berger, and issue any other relief necessary to serve the ends of justice.

Respectfully submitted,

_____/s/_____
Sabrina Shroff, Esq.
Edward Zas, Esq.
Attorneys for Joshua Schulte