

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA : 14 Cr. 68 (KBF)

- against - :

ROSS ULBRICHT, :

Defendant. :

-----X

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT
ROSS ULBRICHT’S POST-TRIAL MOTIONS

Joshua L. Dratel
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732 - 0707
jdratel@joshuadratel.com

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis
Joshua J. Horowitz

TABLE OF CONTENTS

Table of Contents..... i

Table of Authorities..... iii

Introduction. 1

Statement of Facts. 1

ARGUMENT

POINT I

MR. ULBRICHT SHOULD BE GRANTED
A NEW TRIAL BECAUSE THE GOVERNMENT
FAILED TO PROVIDE EXCULPATORY MATERIAL
AND INFORMATION IN A TIMELY MANNER,
THEREBY DENYING HIM HIS FIFTH AMENDMENT
RIGHT TO DUE PROCESS AND A FAIR TRIAL..... 2

A. *The Applicable Law Regarding Brady Material*. 2

 1. *General Principles Governing the Government’s
 Brady Disclosure Obligations*. 2

 2. *The Timing of the Government’s Brady Disclosure Obligations*..... 7

 3. *The Manner of the Government’s Brady Disclosure Obligations*. 9

B. *The Government First Disclosed a Substantial Volume of Brady Material
 Within Voluminous 3500 Material Produced So Close In Time to Trial
 That the Defense Could Not Make Effective Use of the Information*..... 10

C. *The Government’s Untimely Disclosure of Brady Material Was
 Aggravated By Its Late and Continued Production of a Significant
 Volume of Exhibits Throughout the Trial* 12

POINT II

MR. ULBRICHT’S MOTION TO SUPPRESS EVIDENCE
SHOULD BE REOPENED BASED ON INFORMATION
PRODUCED BY THE GOVERNMENT IN CONNECTION
WITH TRIAL, AND SHOULD BE GRANTED IN ITS ENTIRETY. 15

POINT III

THE PROFFER FROM ANDREAS M. ANTONOPOULOS
REGARDING HIS PROPOSED EXPERT TESTIMONY. 17

Conclusion. 28

TABLE OF AUTHORITIES

CASES

Berger v. United States, 295 U.S. 78 (1935) 2, 6

Brady v. Maryland, 373 U.S. 83 (1963) 2-12

Cone v. Bell, 556 U.S. 449 (2009) 3-6, 11

DiSimone v. Phillips, 461 F.3d 181 (2d Cir. 2006) 6

Giglio v. United States, 405 U.S. 150 (1972) 3

Grant v. Alldredge, 498 F.2d 376 (2d Cir.1974) 8

Kyles v. Whitley, 514 U.S. 419 (1995) 2-6

Lambert v. Beard, 537 Fed.Appx. 78 (3d Cir. 2013), *after remand by*
Wetzel v. Lambert, ___ U.S. ___, 132 S. Ct. 1195 (2012),
vacating and remanding 633 F.3d 126 (3d Cir. 2011) 5, 11

Leka v. Portuondo, 257 F.3d 89 (2d Cir.2001) 8, 11

Moore v. Illinois, 408 U.S. 786 (1972) 4

St. Germain v. United States, Nos. 03–cv–8006 (CM), 99–cr–339
 (CM), 2004 WL 1171403 (S.D.N.Y. May 11, 2004) 8

Strickler v. Greene, 527 U.S. 263 (1999) 3-5

United States v. Agurs, 427 U.S. 97 (1976) 6

United States v. Avellino, 136 F.3d 249 (2d Cir. 1998) 7

United States v. Bagley, 473 U.S. 667 (1985) 3, 6

United States v. Blackley, 986 F.Supp. 600 (D.D.C. 1997) 6

United States v. Breit, 767 F.2d 1084 (4th Cir.1985) 9

United States v. Certified Environmental Services, Inc., 753 F.3d 72 (2d Cir. 2014) 2-5, 9

United States v. Coppa, 267 F.3d 132 (2d Cir. 2001) 3-5, 7, 8

United States v. Gil, 297 F.3d 93 (2d Cir. 2002) 9

United States v. Hsia, 24 F.Supp.2d 14 (D.D.C.1998) 3, 6-7, 10

United States v. Jackson, 345 F.3d 59 (2d Cir.2003) 4

United States v. Mahaffy, 693 F.3d 113 (2d Cir.2012) 3

United States v. Pollack, 534 F.2d 964 (D.C. Cir. 1976) 7

United States v. Rittweger, 524 F.3d 171 (2d Cir.2008) 9

United States v. Skilling, 554 F.3d 529 (5th Cir.2009),
aff'd in part and vacated in part on other grounds, 561 U.S. 358 (2010) 9

United States v. Tarantino, 846 F.2d 1384 (D.C.Cir. 1988) 7

United States v. Thomas, 981 F. Supp.2d 229 (S.D.N.Y. 2013) 2-9, 11

United States v. Washington, 294 F. Supp.2d 246 (D. Conn.2003) 8

STATUTES

U.S. Const. Amend. X. 2

U.S. Const. Amend. XIV. 3

18 U.S.C. §3500 1, 7

Rule 16, Fed.R.Crim.P. 14

Rule 33, Fed.R.Crim.P. 1, 2, 28

OTHER

ABA Model Rule of Professional Conduct 3.8(d) (2008). 3

Introduction

This Memorandum of Law is submitted on behalf of defendant Ross Ulbricht in support of his motion for a new trial, pursuant to Rule 33, Fed.R.Crim.P., and to renew his motion(s) to suppress the fruits of certain searches and seizures performed by the government.

As detailed below in POINT I, the Rule 33 motion is premised upon the government's failure to provide exculpatory material in a timely manner. The application in POINT II to renew the suppression motion(s) is based on information learned during trial, either through testimony or material produced by the government pursuant to 18 U.S.C. §3500 (hereinafter "3500 material"). Also, POINT III includes the proffer, summarized in defense counsel's oral presentation in court February 2, 2015, with respect to the proposed defense expert Andreas M. Antonopoulos, whose testimony was precluded.

Accordingly, for the reasons set forth below, as well as in the sealed letter submitted in as part of this motion, it is respectfully submitted that Mr. Ulbricht's motions be granted in their entirety.

Statement of the Facts

Having presided over the entire case, including trial, the Court is cognizant of the relevant facts of this case. Therefore, rather than set forth a separate statement of facts, this Memo of Law will incorporate the relevant facts within each respective Point.

ARGUMENT

POINT I

MR. ULBRICHT SHOULD BE GRANTED A NEW TRIAL BECAUSE THE GOVERNMENT FAILED TO PROVIDE EXCULPATORY MATERIAL AND INFORMATION IN A TIMELY MANNER, THEREBY DENYING HIM HIS FIFTH AMENDMENT RIGHT TO DUE PROCESS AND A FAIR TRIAL

Mr. Ulbricht's Rule 33 motion for a new trial should be granted because the government failed to produce exculpatory material in a timely fashion that would have permitted the defense effective use of the material and information at trial. As a result, as set forth below, the government deprived Mr. Ulbricht of his Fifth Amendment right to Due Process.

A. *The Applicable Law Regarding Brady Material*

1. *General Principles Governing the Government's Brady Disclosure Obligations*

It is well-settled that "[d]ue process requires the Government to provide a criminal defendant with favorable material evidence in its possession." *United States v. Thomas*, 981 F. Supp.2d 229, 232 (S.D.N.Y. 2013), *citing Brady v. Maryland*, 373 U.S. 83, 86 (1963). As the Court in *Thomas* recognized, "[t]he *Brady* rule safeguards the fundamental principal that a trial is a search for the truth[,] and "protects the Government's unique interest in a criminal prosecution 'not [to] win a case, but [ensure] that justice shall be done.'" 981 F. Supp.2d at 232, *quoting Berger v. United States*, 295 U.S. 78, 88 (1935). *See also* 981 F. Supp.2d at 233 ("[w]hen *Brady* material is withheld, the Government's case is 'much stronger, and the defense case much weaker, than the full facts would have suggested'"), *citing Kyles v. Whitley*, 514 U.S. 419, 429 (1995).

As the Second Circuit explained most recently in *United States v. Certified*

Environmental Services, Inc., 753 F.3d 72 (2d Cir. 2014), “[u]nder *Brady* and its progeny, ‘the Government has a constitutional duty to disclose favorable evidence to the accused where such evidence is ‘material’ either to guilt or to punishment.’” *Id.*, at 91, quoting *United States v. Coppa*, 267 F.3d 132, 139 (2d Cir. 2001).¹

In turn, “[f]avorable evidence includes not only evidence that tends to exculpate the accused, but also evidence that is useful to impeach the credibility of a government witness.” *Id.* See also *Strickler v. Greene*, 527 U.S. 263, 281-82 (1999); *United States v. Bagley*, 473 U.S. 667, 676-77 (1985); *Giglio v. United States*, 405 U.S. 150, 154-55 (1972); *United States v. Mahaffy*, 693 F.3d 113, 127 (2d Cir.2012); *Thomas*, 981 F. Supp.2d at 238; *United States v. Hsia*, 24 F.Supp.2d 14, 29 (D.D.C.1998).

Regarding the other prong by which *Brady* material is defined, in *Certified*

¹ In *Cone v. Bell*, 556 U.S. 449 (2009), a majority of the Court noted that

[a]lthough the Due Process Clause of the Fourteenth Amendment, as interpreted by *Brady*, only mandates the disclosure of material evidence, the obligation to disclose evidence favorable to the defense may arise more broadly under a prosecutor's ethical or statutory obligations. See *Kyles*, 514 U.S., at 437 (“[T]he rule in [*United States v. Bagley*, 473 U.S. 667 (1985)] (and, hence, in *Brady*) requires less of the prosecution than the ABA Standards for Criminal Justice Prosecution Function and Defense Function 3–3.11(a) (3d ed.1993)”). See also ABA Model Rule of Professional Conduct 3.8(d) (2008) (“The prosecutor in a criminal case shall” “make timely disclosure to the defense of all evidence or information known to the prosecutor that tends to negate the guilt of the accused or mitigates the offense, and, in connection with sentencing, disclose to the defense and to the tribunal all unprivileged mitigating information known to the prosecutor, except when the prosecutor is relieved of this responsibility by a protective order of the tribunal”).

556 U.S. at 470.

Environmental Services the Second Circuit pointed out that

“evidence is ‘material’ within the meaning of *Brady* when there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different,” such that the failure to disclose “‘undermine[s] confidence in the verdict.’” *Cone v. Bell*, 556 U.S. 449, 469-70 (2009), quoting *Kyles v. Whitley*, 514 U.S. 419, 435 (1995).

753 F.3d at 91.

In that context,

“[t]here are three components of a true *Brady* violation: (1) The evidence at issue must be favorable to the accused, either because it is exculpatory or because it is impeaching; (2) that evidence must have been suppressed by the [Government], either willfully or inadvertently; and (3) prejudice must have ensued.” *United States v. Jackson*, 345 F.3d 59, 71 (2d Cir.2003), quoting *Strickler v. Greene*, 527 U.S. 263, 281-82 (1999).

753 F.3d at 91. See also *Thomas*, 981 F. Supp.2d at 238, citing *United States v. Coppa*, 267 F.3d at 140 and *Moore v. Illinois*, 408 U.S. 786, 794-95 (1972).

Again drawing on *Coppa*, the Court in *Certified Environmental Services* commented that “[a]lthough the government’s obligations under *Brady* may be thought of as a constitutional duty arising before or during the trial of a defendant, the scope of the government’s constitutional duty . . . is ultimately defined retrospectively, by reference to the likely effect that the suppression of particular evidence had on the outcome of the trial.” 753 F.3d at 92, quoting *Coppa*, 267 F.3d at 140.

Thus, the Circuit added in *Certified Environmental Services*, “‘strictly speaking, there is never a real ‘*Brady* violation’ unless the [Government’s] nondisclosure was so serious that there is a reasonable probability that the suppressed evidence would have produced a different

verdict.” 753 F.3d at 92, *quoting Strickler*, 527 U.S. at 281.

The Court in *Certified Environmental Services* elaborated that

[t]his aspect of *Brady* affects not only what the Government is obligated to disclose, but when it is required to do so. Temporally, “the timing of a disclosure required by *Brady* is . . . dependent upon the anticipated remedy for a violation of the obligation to disclose: the prosecutor must disclose . . . exculpatory and impeachment information no later than the point at which a reasonable probability will exist that the outcome would have been different if an earlier disclosure had been made.”

753 F.3d at 92, *quoting Coppa*, 267 F.3d at 142.

The standard for the inquiry regarding prejudice, as the Supreme Court explicated in *Kyles v. Whitley*, asks “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.” 514 U.S. at 434. *See also Lambert v. Beard*, 537 Fed.Appx. 78, 87 (3d Cir. 2013), *after remand by Wetzel v. Lambert*, ___ U.S. ___, 132 S. Ct. 1195 (2012), *vacating and remanding* 633 F.3d 126 (3d Cir. 2011).

As the Court in *Kyles* noted, “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 . . . [M]ateriality is a ‘reasonable probability’ of a different result, and the adjective is important.” 514 U.S. at 434 (internal citations omitted). *See also Thomas* 981 F. Supp.2d at 242-43.

The Courts have also encouraged prosecutors to err on the side of disclosure for reasons of prudence as well as fairness. As the Court in *Cone v. Bell* cautioned, “[a]s we have often observed, the prudent prosecutor will err on the side of transparency, resolving doubtful

questions in favor of disclosure.” 556 U.S. at 470, *citing Kyles*, 514 U.S., at 439; *Bagley*, 473 U.S. 667, 711, n. 4 (Stevens, J., *dissenting*); *United States v. Agurs*, 427 U.S. 97, 108 (1976).

As the Court in *Thomas* recognized, “questions about the reliability of [] exculpatory information” are judgment calls for [a defendant] and his counsel, not the Government; ‘to allow otherwise would be to appoint the fox as henhouse guard.’” 981 F. Supp.2d at 241, *quoting DiSimone v. Phillips*, 461 F.3d 181, 195 (2d Cir. 2006).

Thus, in contemplating whether and when to disclose, “[t]he government must bear in mind, however, that it has the ‘affirmative duty to resolve doubtful questions in favor of disclosure,’ and that ‘if the sword of Damocles is hanging over the head of one of the two parties, it is hanging over the head of the [government].’” *Hsia*, 24 F. Supp.2d at 30, *quoting United States v. Blackley*, 986 F.Supp. 600, 607 (D.D.C. 1997) (internal quotations omitted).

Also binding the government is the particular role the prosecutor plays in the criminal justice system. As the Supreme Court reaffirmed in *Cone v. Bell*, “[a]lthough the State is obliged to ‘prosecute with earnestness and vigor,’ it ‘is as much [its] duty to refrain from improper methods calculated to produce a wrongful conviction as it is to use every legitimate means to bring about a just one.’” *Cone v. Bell*, 556 U.S. at 469, *quoting Berger*, 295 U.S. at 88.

The Court in *Hsia*, in deciding pretrial motions, added that

[m]ore fundamentally, the government would do well to remember that “the prosecutor’s role transcends that of an adversary: he [or she] ‘is the representative not of an ordinary party to a controversy, but of a sovereignty. . . . whose interest . . . in a criminal prosecution is not that it shall win a case, but that justice shall be done.’”

24 F. Supp.2d at 30, *quoting Bagley*, 473 U.S. at 675 n. 6 (*quoting Berger*, 295 U.S. 78).

2. *The Timing of the Government’s Brady Disclosure Obligations*

Even when exculpatory is disclosed, a *Brady* violation can still occur if the disclosure is untimely. As the Court in *Thomas* stated, “[e]vidence is suppressed when the prosecutor does not disclose it “in time for its effective use at trial.” 981 F. Supp.2d at 239, quoting *Coppa*, 267 F.3d at 135 (internal citations omitted), and citing *United States v. Avellino*, 136 F.3d 249, 255 (2d Cir. 1998).

Moreover, delaying disclosure until it is contemporaneous with production of 3500 material does not absolve the government of its responsibility to disclose exculpatory material and information in time for the defense’s effective use at trial. As the Court in *Hsia* recognized, “the existence of a duty to disclose witness statements at trial pursuant to the Jencks Act, 18 U.S.C. §3500, does not eviscerate the government’s *Brady* obligation to disclose witness statements well in advance of trial if portions of those statements also fall under *Brady*.” 24 F. Supp.2d at 29, citing *United States v. Tarantino*, 846 F.2d 1384, 1414 n. 11 (D.C.Cir. 1988).

As the Court in *Hsia* pointed out, “[t]his is important because the government is required to disclose *Brady* material in sufficient time for the defendant to ‘use the favorable material effectively in the preparation and presentation of its case,’ *United States v. Pollack*, 534 F.2d 964, 973 (D.C.Cir. 1976), while Jencks material is not required to be disclosed until after the witness has testified.” 24 F. Supp.2d at 29. See also *Thomas*, 981 F. Supp.2d at 241 (“[t]he Government’s argument conflates its Jencks Act and *Brady* obligations. While those responsibilities overlap at times, they are distinct legal concepts. The Jencks Act is concerned with discovery to be produced by the Government. *Brady* is concerned with fairness”).

The Court in *Thomas* further recognized a reactive defense maneuver “after a late *Brady*

disclosure is no substitute for thoughtful preparation and a considered strategy. *Brady* material must be provided to a defendant “in time for its *effective* use at trial.” 981 F. Supp.2d at 242, quoting *Coppa*, 267 F.3d at 135 (emphasis supplied by Court in *Thomas*), and citing *Grant v. Alldredge*, 498 F.2d 376, 382 (2d Cir.1974) (refusing to “infer from the failure of defense counsel, when surprised at trial, to seek time to gather other information on [the suppressed witness], that defense counsel would have by-passed the opportunity had the prosecutor apprised him of the [evidence] at a time when the defense was in a reasonable pre-trial position to evaluate carefully all the implications of that information”).

As the Second Circuit explained in *Leka v. Portuondo*, 257 F.3d 89 (2d Cir.2001), “[t]he opportunity for use under *Brady* is the opportunity for a responsible lawyer to use the information with some degree of calculation and forethought.” *Id.*, at 101-03. See also *Thomas*, 981 F. Supp.2d at 240; *St. Germain v. United States*, Nos. 03-cv-8006 (CM), 99-cr-339 (CM), 2004 WL 1171403, at *18 (S.D.N.Y. May 11, 2004) (“defense strategies are largely formed prior to trial ... and the necessary predicate is that the strategies selected were chosen after careful consideration of all constitutionally-compelled disclosure”).

Consequently, as the Court in *Leka* realized,

[w]hen such a disclosure is first made on the eve of trial, or when trial is under way, the opportunity to use it may be impaired. The defense may be unable to divert resources from other initiatives and obligations that are or may seem more pressing. And the defense may be unable to assimilate the information into its case.

257 F.3d at 101, citing *United States v. Washington*, 294 F. Supp.2d 246, 250 (D. Conn.2003) (government’s failure to disclose evidence impeaching the central witness until after the first day of trial prejudiced defendant because the late disclosure prevented defense counsel from

investigating and planning overall trial strategy). *See also Thomas*, 981 F. Supp.2d at 242.

Indeed, even in *Certified Environmental Services*, in which the Court did not find a *Brady* violation because, *inter alia*, the notes at issue “were at best marginally helpful to the defense[,]” 753 F.3d at 93, and the undisclosed reference in the notes “was not inconsistent with [the prior] testimony[,]” *id.*, the Court nevertheless added that

[t]his is not to suggest, however, that the prosecutors did nothing wrong in failing to disclose [the] handwritten notes along with the typewritten summaries. To begin with, we see no reason – and the Government offers none – why the prosecutors here could not and should not have “acted in favor of disclosing the *Brady* material earlier.”

Id., quoting *United States v. Rittweger*, 524 F.3d 171, 182 (2d Cir.2008).

3. The Manner of the Government’s *Brady* Disclosure Obligations

In *Thomas*, the Court also emphasized “the importance of the manner of the Government’s disclosure.” 981 F. Supp.2d at 240, *citing United States v. Gil*, 297 F.3d 93, 106 (2d Cir. 2002) (labeling *Brady* evidence as 3500 material and producing it as part of a large 3500 production on the eve of trial constitutes suppression), and *United States v. Breit*, 767 F.2d 1084, 1090 n. 4 (4th Cir.1985) (government may not discharge its *Brady* obligation merely by tendering a witness without providing any indication that the witness’s testimony may be helpful to defense).

In that context, “the Government cannot hide *Brady* material as an exculpatory needle in a haystack of discovery materials.” 981 F. Supp.2d at 239, *citing United States v. Skilling*, 554 F.3d 529, 577 (5th Cir.2009), *aff’d in part and vacated in part on other grounds*, 561 U.S. 358 (2010) (suggesting that *Brady* violations related to voluminous open file discovery depend on

“what the government does in addition to allowing access to a voluminous open file”). *See also United States v. Hsia*, 24 F.Supp.2d 14, 29-30 (D.D.C.1998) (“[g]overnment cannot meet its *Brady* obligations by providing . . . 600,000 documents and then claiming that [the defendant] should have been able to find the exculpatory information”).

B. *The Government First Disclosed a Substantial Volume of Brady Material Within Voluminous 3500 Material Produced So Close In Time to Trial That the Defense Could Not Make Effective Use of the Information*

Here, within the 5,000 pages of 3500 material for the government’s first witness, Homeland Security Investigations Special Agent Jared Der-Yeghiayan, produced less than two weeks prior to trial – and, in some instances, 30 months after the information was memorialized by SA Der-Yeghiayan (and in most instances, close to or more than two years after) – a substantial volume of exculpatory material and information.² Other exculpatory material was included within the 3500 material for Internal Revenue Special Agent Gary Alford (which was produced January 6, 2015).

Attached as Exhibit 1 hereto is a catalog of the 3500 material that is exculpatory, and which was not disclosed prior to the serial productions of 3500 material – the evening of December 31, 2014, and the evening of January 6, 2015. As Exhibit 1 demonstrates, 70 separate documents (some consisting of multiple pages) in the 3500 material contained exculpatory material and information that was not provided to the defense at a time in which it could be used effectively at trial.

In addition, there were substantial redactions within the 3500 material. While ordinarily

² In addition, as set forth in the sealed letter accompanying this motion, the government committed two separate, independent *Brady* violations both prior to and during trial.

that might not be cause for concern, in this instance it is manifest from comparison of sections of SA Der-Yeghiayan's 3500 material that some of the redactions (for instance, in Report 54) were of exculpatory information about an alternative perpetrator (that was unredacted from a mirror document produced as part of his 3500 material). As a result, the redactions should be examined for additional exculpatory material and information that was not disclosed to the defense at all.

Also, SA Alford's 3500 material references interviews conducted by law enforcement at or around the time of Mr. Ulbricht's arrest. Upon information and belief, those interviews – of Mr. Ulbricht's friends and others acquainted with him – generated exculpatory material and information. Yet none of those interviews have been produced to the defense in any form.

Nor can it be disputed that the information cited in Exhibit 1 constitutes *Brady* material. *See Leka v. Portuondo*, 257 F.3d at 99 (*Brady* material is “of a kind that would suggest to any prosecutor that the defense would want to know about it”). *See also Thomas* 981 F. Supp.2d at 238-39. Indeed, in *Lambert v. Beard*, 537 Fed.Appx. 78, 81-82 (3d Cir. 2013), the nondisclosure related to notes reflecting that “unbeknownst to either the defense or the jury at the time, [a critical government witness] had in fact supplied police with another perpetrator”). *See also Cone v. Bell*, 556 U.S. at 471 (undisclosed investigative reports containing information consistent with defense theory were deemed *Brady* material).

Here, as well, the cumulative effect of the untimely disclosure amplified its impact and prejudice suffered by Mr. Ulbricht as a result. *See Cone v. Bell*, 556 U.S. at 475 (“[i]t is possible that the suppressed evidence, viewed cumulatively, may have persuaded the jury” not to impose the death sentence on the defendant) (footnote omitted); *id.*, at 471 (“both the quantity and the quality of the suppressed evidence lends support to” the defendant's position).

C. *The Government's Untimely Disclosure of Brady Material Was Aggravated By Its Late and Continued Production of a Significant Volume of Exhibits Throughout the Trial*

The government's late disclosure of *Brady* material was compounded by its addition of hundreds of additional exhibits after the December 3, 2014, deadline for the production of Government Exhibits to the defense, and the modification of more than 200 other Government Exhibits. That continued fluidity in the government's presentation – in a trial focused on exhibits rather than testimony – created for practical and legal purposes a continuously moving target.

In fact, what began as only a few new exhibits – fewer than ten – trickling in December 5, 2014, two days after the government's exhibit deadline, quickly snowballed into dozens of exhibits being added or modified every few days, with a total of approximately 230 new exhibits added after the deadline for Government Exhibits, and the modification of 50-60% of the Exhibits included in the government's initial list.³

Nor does that take into account the approximately 40 Government Exhibits that were simply removed by the government after its initial Exhibit list was provided, or the modifications to the same Exhibits multiple times. For example, metadata added to the 200 series January 7, 2015, and then subsequently reformatted for the entire 200 series January 20, 2015, a week into

³ Any imprecision in the number of government exhibits added or modified after the initial deadline for Government Exhibits is a result of the manner in which additional or modified exhibits were provided to the defense. For instance, some exhibits were provided only in hard copy during the trial day, which has made the date of their production difficult to verify (and difficult as well to identify at all in some instances). Still others were provided in bulk or in the context of sweeping revisions which blurred the lines between new and modified exhibits, and in some of these instances, an accounting of the new versus modified exhibits was not provided by the government. Attached hereto as Exhibit 2 is a chart which tracks the additions, modifications and other changes to the Government's Exhibits, to the extent we were able to document them.

trial.

Indeed, between December 31, 2014, when the government began to produce 3500 material to the defense – commencing with a 5,000-page production for its first witness, Special Agent Jared Der-Yeghiayan – and the start of the trial, January 12, 2015, the defense was saddled with an overwhelming number of new and modified exhibits. In total, the government produced approximately 145 new exhibits during that time period, and modified between 50 and 100 others.

The January 7, 2015, changes to the exhibit list alone were so voluminous and convoluted that defense counsel required a separate e-mail from the government listing the changes item by item in order to decipher them. The resultant January 8, 2015, e-mail from Assistant United States Attorney Serrin Turner, explaining the changes, was several paragraphs long. In it, the government identified a total of 130 new exhibits (not including an additional approximately ten new exhibits that defense counsel later discovered that were not listed in the government’s e-mail).

Other changes to the exhibit list included confusing modifications, such moving Google chat transcripts, formerly in the 300 series, to the (new) 1000 series, and the replacement of Torchat transcripts included in the prior exhibit list with new exhibits containing some chats “broken up into smaller excerpts (or related sets of excerpts), with each made into a separate exhibit,” other chats in which “some material has been deleted from the chats[,]” and “some exhibits contain[ing] new chat excerpts not included in [the government’s] earlier set of exhibits.” *See* January 8, 2015, e-mail from Serrin Turner to Joshua L. Dratel, Esq., Lindsay A. Lewis, Esq., and Joshua J. Horowitz, Esq, a copy of which is attached hereto as Exhibit 3.

The government also explained in that e-mail that “[m]etadata has been added to many of the exhibits in the 100 & 200 series” while still other exhibits had “simply been renumbered.”

Id. Defense counsel also discovered, through meticulous review of the government’s revised Exhibit list, that the government had removed 31 exhibits from its initial list.

During this same pre-trial time frame, the defense was also provided additional discovery January 2, 2015, pursuant to Rule 16, Fed.R.Crim.P., in the form of 19 Google voice mail messages from Mr. Ulbricht to government witness Richard Bates, one of which was added as a Government Exhibit (GX 1005), but only weeks later, and well into trial.

In fact, the number of new Government Exhibits nearly doubled in volume *after* trial started, with many of those new exhibits provided to the defense only minutes or hours before court began session, or before they would be introduced by the government through a particular witness. For instance, in just the final week of the government’s case, between January 25, 2015, and January 28, 2015, the government produced to defense counsel for the first time approximately 44 new exhibits.

Many of these exhibits first revealed to the defense in the 11th hour of the government’s case, and namely those in the 600 series, turned over January 28, 2015 – which included GX 620, a 63-page spreadsheet of thousands of transactions – were to be introduced and used in conjunction with former Special Agent Ilhwan Yum’s testimony regarding the bitcoin wallet analysis he had only begun and completed during the course of the trial.

The defense had not even been made aware of any bitcoin wallet analysis, let alone provided with related exhibits, until 10:17 p.m. the night of January 25, 2015, when a 3MB excel spreadsheet, which contained the wallet analysis conducted by former SA Yum, was provided to

defense counsel. At that time the government also notified defense counsel that the government intended to produce the spreadsheet as 3500 material, and was in the process of preparing a series of summary exhibits, based on the spreadsheet, to be introduced during former SA Yum's testimony.⁴

Accordingly, for all the reasons set forth above, and in Mr. Ulbricht's prior submissions and oral argument, it is respectfully submitted that his Rule 33 motion for a new trial should be granted in its entirety.

POINT II

MR. ULBRICHT'S MOTION TO SUPPRESS EVIDENCE SHOULD BE REOPENED BASED ON INFORMATION PRODUCED BY THE GOVERNMENT IN CONNECTION WITH TRIAL, AND SHOULD BE GRANTED IN ITS ENTIRETY

The 3500 material produced by the government just prior to trial also revealed information critical to Mr. Ulbricht's initial suppression motion, and which requires the Court to reopen Mr. Ulbricht's suppression motion and to grant it in its entirety on the basis of this information, or at the very least conduct an evidentiary hearing.

The predominant share of the documents necessitating the reopening of Mr. Ulbricht's suppression motion were included in the 3500 material produced in regard to SA Der-Yeghiayan. In particular, text messages between SA Der-Yeghiayan and a confidential informant (designated in the 3500 material and hereinafter as "CI") demonstrate unequivocally that the government was conducting warrantless TOR network surveillance on a TOR exit node that would have enabled

⁴ A disk containing the documents that would ultimately become GX 650 and 651 was also first provided to defense counsel the night of January 25, 2015.

the government to capture information about the source and content of the data passing through the TOR exit node. *See* 3505-4059 to 3505-4066.

For example, in an August 4, 2012, communication, at 2:13 p.m., SA Der-Yeghiayan asked the CI, “[a]re we up on the exit node yet?” In response, at 7:18 p.m., August 12, 2012, the CI states “[s]uccess!” and then, at 7:20 p.m., “100 percent running, logging, and recording . . . with verification.” *Id.*, at 3505-4059 to 3505-4060.⁵

In the context of Mr. Ulbricht’s suppression motion, this surveillance raises some novel Fourth Amendment issues, and also provides further evidence that the government discovered the Internet Protocol (hereinafter “IP”) address for the Iceland server ending in “.49” through warrantless TOR network surveillance.

In addition, still other text messages between SA Der-Yeghiayan and the CI discuss the prospect of the government performing a distributed denial of service (hereinafter “DDOS”) attack on the Silk Road server, with the express purpose of “listening” to the Silk Road servers. *See* 3505-4066. While it is not clear from the context of the text messages whether the government ever performed the DDOS attack discussed, it is known, from evidence in the record, that DDOS attacks on the Silk Road servers did occur, including one during the Spring of 2013, when the government was actively seeking to find the Silk Road servers, and during which period the government claimed to determine the IP address of the Iceland server by other means.

As a result, Mr. Ulbricht’s suppression motion(s) should be reopened to explore whether it was the government that conducted (or authorized) those DDOS attacks, and whether the

⁵ In fact, at other points in SA Der-Yeghiayan’s 3500 material, at 3505-315 and 3505-344, SA Der-Yeghiayan noted that the Silk Road server IP addresses were unknown and were almost impossible to locate *because of TOR*.

government was able to gain access to the Silk Road servers in that manner.

Moreover, in SA Der-Yeghiayan's 3500 material, there is evidence of additional pen registers not disclosed or produced to the defense. For instance, an e-mail from former Special Agent Christopher Tarbell has the subject "email pen." *See* 3505-661-62. The message is redacted, however, so it is not known for certain whether this refers to surveillance of an e-mail account, or accounts, of Mr. Ulbricht's that the government failed to produce in discovery, or whether a pen register for emails was ever sought. In reopening Mr. Ulbricht's suppression motion, the government should be required to produce any and all pen registers not previously provided to defense counsel, such as any for Mr. Ulbricht's e-mail accounts.

Accordingly, based on the information provided to the defense in the context of 3500 material and for the reasons set forth herein, Mr. Ulbricht's suppression motion should be reopened and granted in its entirety.

POINT III

THE PROFFER FROM ANDREAS M. ANTONOPOULOS REGARDING HIS PROPOSED EXPERT TESTIMONY

As set forth in Lindsay A. Lewis, Esq.'s January 31, 2015, letter to the Court, proposed defense expert witness Andreas M. Antonopoulos was on a plane from Germany to the United States at the time Mr. Ulbricht's supplemental submission to the Court regarding Mr. Antonopoulos's testimony was due.

Thus, Mr. Ulbricht was unable to provide the Court with a written proffer regarding the expected content of Mr. Antonopoulos's testimony at that time. For the same reason, Mr. Ulbricht did not have the ability, in that letter, to provide the Court with the full range of Mr.

Antonopoulos's qualifications and credentials.

Had Mr. Antonopoulos been permitted to testify at Mr. Ulbricht's trial, he would have testified (as outlined in defense counsel's oral presentation the morning of February 2, 2015), as follows:

- *Introduction.* Bitcoin superficially resembles cash and its accounting, as presented on sites like blockchain.info, superficially resembles a bank account statement. Bitcoin, however, operates in a way that is fundamentally different to either cash or bank accounts. These nuanced differences are not readily apparent to the layperson. Ignoring these differences can lead to erroneous conclusions about balances, flows, and accounting. While laypeople can readily understand the use of bitcoin for simple transactions, like purchasing a cup of coffee, that understanding cannot be extended to forensic analysis without detailed explanation of features unique to bitcoin.
- *Change Addresses.* Unlike bank accounts, bitcoin transactions cannot "withdraw" arbitrary amounts from an "account." A bitcoin wallet will typically contain many addresses with varying amounts of bitcoin in them – like a wallet with cash and change inside. A bitcoin transaction can only spend from a set of transaction outputs as recorded by previous transactions, it can only spend the denominations it has within the wallet. This means, for example, that if a bitcoin address has previously received 5 bitcoin, as the output of a previous transaction, a subsequent transaction can only spend the entire 5 bitcoin. In order to spend smaller amounts, a transaction must be constructed to return "change" back to the originating

wallet. For example, to make a payment of 1 bitcoin using a previously recorded 5 bitcoin output, a transaction would be constructed as follows:

transaction input from address A: 5 bitcoin,

transaction output to address B: 1 bitcoin,

transaction output to address C: 4 bitcoin.

Many bitcoin wallets automatically generate unique change addresses for each transaction, which are different from the originating address. In the example above, address C is different from address A, but is a change address belonging to the same wallet.

- *Erroneously Reported Transaction Values Are A Known Weakness.* It is important to note that there is nothing to distinguish the principal payment from the change in the transaction itself. In fact, popular software systems such as blockchain.info attempt to calculate and report the value of a transaction by guessing which of the addresses is a principal payment and which is change. Because the transaction itself does not identify change addresses, the reported transaction value is sometimes incorrect presenting the change as the value itself. In the example above, blockchain.info might report this transaction as having a value of 4 bitcoin instead of its true value of 1 bitcoin.

When multiple transactions are aggregated, as flows in and out of a single address, as is the case with blockchain.info's address view, this error can be compounded in such a way that the summary presented at the top of the page significantly overestimates the sum of payments. This is a known weakness of any software

that attempts to provide accounting without the context of change addresses.

- *Accurate Forensic Analysis of Flows Must Include Change Addresses with Zero Balances.* It is common practice in the bitcoin industry to avoid the reuse of addresses, for privacy and security reasons. This applies to both the use of primary addresses, *i.e.*, those used to receive payments, as well as change addresses, *i.e.*, those generated only for receiving change. Even when a user reuses a primary address for convenience, their wallet software may automatically generate new unique change addresses for each transaction. As a result, change addresses are often only used twice – once to receive change and once more to make a subsequent payment depleting the balance to zero. Unlike bank accounts, bitcoin wallets that are frequently used may contain thousands of transient change addresses, the vast majority of which have a zero balance. While these empty change addresses are no longer relevant for the calculation of the current balance of a user’s wallet, they are of critical importance when attempting to reconstruct an accounting of the total flow between wallets. Omitting these change addresses from such a calculation may lead to double-counting and inflating the estimated totals transacted between two parties.
- *Accurate Forensic Analysis of Flows Must Include More Than One-To-One Transactions.* Most transactions include change. In fact, the only transactions that do not include change (one-to-one transactions) are those where the indivisible input amount coincidentally matches the sum of the principal payment and transaction fee. In other words, unless the wallet contains “exact change” to make

the desired payment and cover the transaction fee. Most transactions by necessity, combine several inputs or use a larger input and contain several outputs including change. As a result, one-to-one transactions are the exception rather than the rule. *See Ulbricht Trial Transcript*, January 29, 2015, at 1727 (Mr. Dratel: Q. Did you do any analysis of transactions from the Silk Road server bitcoin addresses to the Ross Ulbricht laptop addresses that were not one-to-one transactions? Mr. Yum: A. No, I did not.).

- *Double Counting Both Ways.* If change addresses are omitted from the calculation of flows between two wallets, the error previously described can accumulate on both sides of the flow (outgoing and incoming). In other words, if both the Silk Road wallet and Mr. Ulbricht's wallet generate single-use change addresses, the omission of those addresses from analysis would lead to an accumulation of error that grossly overstates the total volume of payments between the wallets.
- *Flawed Methodology.* Analysis of the total payment volume between addresses corresponding to the Silk Road wallet and Mr. Ulbricht's wallet will have a critical dependence on the correct identification of change addresses. Any analysis of the flows between two wallets must account for every address referenced in a transaction and correctly identify its origin and ownership. Incorrect attribution of an address can lead to incorrect calculations of the volume of payments which can accumulate over several transactions, particularly if the flows are bidirectional. Additionally, a methodology that relies on address lists

constructed from non-zero balance addresses at the time of seizure would exclude all transient change addresses from analysis. Thus, the assumption that bitcoin behaves like a bank account and that blockchain.info transaction lists are equivalent to bank statements is not only flawed but when used as the basis for methodology of forensic analysis of transaction flows will inevitably lead to gross miscalculation. This gross miscalculation could appear as a large sum of bitcoin seemingly unaccounted for but which was actually never there to begin with and instead was simply an artifact of double counting.

- *Hot Wallet.* The bitcoin wallets used by individuals differ significantly from those used on bitcoin servers with larger user populations. A server managed wallet, also known as a hot wallet, aggregates the funds of all users of the site as well as the operating funds and profits from the operation of the site itself. Individual user funds are accounted for in the webserver's database separate from the bitcoin wallet. In the bitcoin wallet itself, the funds are commingled. Incoming payments are made to newly generated addresses. The deposit addresses would typically be associated with specific users in the server's database so that these deposits can be correctly attributed. Withdrawals, however, are made from the communal hot-wallet so that a customer depositing and then withdrawing funds will receive the withdrawal from a different address than the deposit address. In this, a hot wallet resembles a bank branch cash reserves, in that a customer depositing and withdrawing cash will not typically receive the same bills.

Analysis of the blockchain by address attribution will show all withdrawals from

such a hot wallet without the ability to distinguish between user withdrawals, merchant withdrawals, operator profit withdrawals, or other payments absent additional analysis of the webserver's internal accounting database.

- *Use of the Marketplace Trading Wallet as a Bank Account.* Services that offer bitcoin accounts for buyers and sellers are often used as quasi-banks by their users. In order to take advantage of short term opportunities to trade with others, users of the service may maintain high balances on the server. While transactions into and out of the server require up to one hour for settlement, transactions between participants on the server take place directly between addresses of the same hot wallet and are therefore instantaneous. If users are acting as currency speculators, the advantage of maintaining a high balance on the server to be able to execute opportunistic speculative trades and take advantage of sudden exchange rate fluctuations is particularly appealing. As a result, currency speculators using a marketplace as an unofficial exchange to trade with other currency speculators will typically maintain a high balance on server for rapid execution of trades as well as large inflows and outflows to and from that account. While the practice of maintaining a large balance on a server-held wallet is helpful for speculative trading, it also represents a security risk. Such funds are not under the direct control of the user and are vulnerable to hack or theft by the operator. It is therefore common, in such cases, to have a large volume of transactions between a user-held wallet and the server-held wallet. When profits are realized on the server, the excess balance is withdrawn. Similarly when losses occur

balances are replenished with a deposit. A series of such transactions will also generate many change addresses which must be accounted for in order to represent an accurate picture of the flow.

- *Ownership, Control and Access.* Assuming that bitcoin addresses are just like bank accounts also leads to another fundamental misunderstanding – that access equals ownership. The use of a bank account conflates ownership, control, and access of the funds to a single individual or at most a few individuals who are joint holders of the account. In bitcoin, ownership, control, and access are fundamentally distinct. Rather than comparing bitcoin addresses to bank accounts, a more accurate analogy would be to compare them to numbered lockers at a public train station. Each locker has a mail slot which allows anyone to deposit any amount into the locker. The lockers are accessible by the public at large, who can walk into the train station and open any locker by entering a PIN number. Knowledge of the PIN confers access but does not imply exclusive control or ownership of that locker. Multiple people may have knowledge of the PIN and therefore access to the lockers contents.

In bitcoin, access does not imply rightful ownership. Continuing with the locker example, some lockers may have PIN numbers that are published and accessible to the public at large allowing anyone who knows the PIN number to access that locker. For example, in my book *Mastering Bitcoin* (O'Reilly Media, December 2014) several bitcoin addresses are used as examples to illustrate different concepts. The private keys that provide access to these bitcoin addresses are

published in the book. This allows students replicating the examples in the book to create transactions with deposits and withdrawals from those addresses. It is impossible to discern whether a transaction was initiated by one user or another. Transactions created by them are indistinguishable as they require only proof of knowledge of the private key. While I can be said to be the “owner” having created these addresses, I cannot be said to have “control” as I do not have exclusive access. Conversely, possession of the private key shown in an example in the book, proves nothing about control or ownership of that address. I am not notified when a student uses the addresses and unless I take proactive steps to monitor the addresses, I have no knowledge of their current balance or past transaction history.

The presence of private keys on a computer narrowly proves the capability of access to those addresses at that exact moment in time. It does not prove access prior to that moment in time. It does not prove exclusivity of access. It does not prove ownership of those addresses or their contents. It does not prove exclusive control over those addresses. Others with access to those private keys have equal and indistinguishable access, as an owner would, regardless of true ownership.

Private keys can exist on a computer device as part of back-ups copied from other computers. Additionally, hackers or others could gain access to a computer device where private keys are stored, copy that data, and thereby obtain access and control over the corresponding addresses without the computer owners’ knowledge.

- *Exchanging large amounts of bitcoin for national currencies (e.g., USD).* The currency exchanges available in the bitcoin industry are still very small. The total liquidity of bitcoin's exchange markets is miniscule in comparison to any stock or currency exchange. As a result, any attempt to exchange large amounts of bitcoin cause extreme fluctuations in value. For analogy, a large trade in USD currency markets is like dropping a rock in the Pacific Ocean, barely causing a ripple. By comparison, the same amount traded in the bitcoin market is like dropping a rock into a small swimming pool, causing a large wave. Such waves are noticed and commented on by the broader bitcoin community. In popular forums, such as reddit or bitcointalk, a large sell-order is called a "sell wall" because it resembles a vertical "wall" in a graphical view of an exchange's order book. The initiator of such a transaction is called a "bearwhale," borrowing the terms "whale" (a market-moving investor) and "bear" (a large seller putting downward pressure on a market). The activities of such traders are the source of much speculation and discussion on trading forums. In simple terms, it is very difficult to make a very large transaction on the limited-liquidity bitcoin markets without being noticed and discussed.

In addition, the following credentials are relevant to Mr. Antonopoulos's qualification as a bitcoin expert:

- Mr. Antonopoulos is the author of *Mastering Bitcoin*, published by O'Reilly Media, the world's leading publisher of computer software and programming books;

- Mr. Antonopoulos appeared as an expert witness for the Senate Committee on Banking Trade and Commerce of the Canadian Senate and testified before the Senate Committee as to bitcoin's legal, regulatory and technological implications;
- Mr. Antonopoulos is a Teaching Fellow at the University of Nicosia where he contributes to the curriculum development and teaches courses as part of university's Masters of Sciences in Digital Currencies; and
- Mr Antonopoulos has consulted for banking and financial services companies, designing incident response policies and computer forensics procedures. In his role as security consultant he has participated in numerous computer security investigations, vulnerability assessments and risk assessments.

Conclusion

Accordingly, for all the reasons set forth above, and in Mr. Ulbricht's prior submissions and oral argument, it is respectfully submitted that his motion for a new trial, pursuant to Rule 33, Fed.R.Crim.P., should be granted, and/or that his motion to suppress evidence be reopened and granted in its entirety.

Dated: 6 March 2015
New York, New York

Respectfully submitted,

/S/ Joshua L. Dratel
JOSHUA L. DRATEL
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707

Joshua J. Horowitz
225 Broadway, Suite 1804
New York, New York 10007
(845) 667-4451

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis
Whitney G. Schlimbach
Joshua J. Horowitz