15-1815-CR

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

ROSS WILLIAM ULBRICHT, AKA DREAD PIRATE ROBERTS, AKA SILK ROAD, AKA SEALED DEFENDANT 1, AKA DPR,

Defendant-Appellant.

On Appeal from the United States District Court for the Southern District of New York (New York City)

APPENDIX
VOLUME III OF VI
Pages A515 to A768

MICHAEL A. LEVY
SERRIN A. TURNER
ASSISTANT UNITED STATES ATTORNEYS
UNITED STATES ATTORNEY'S OFFICE FOR THE SOUTHERN DISTRICT OF NEW YORK
Attorneys for Appellee
1 Saint Andrew's Plaza
New York, New York 10007
212-637-2346

JOSHUA L. DRATEL, P.C.
Attorneys for Defendant-Appellant
29 Broadway, Suite 1412
New York, New York 10006
212-732-0707

Table of Contents

Page

Volume I

Table of Contents
(Continued)

Page

Volume II

Table of Contents
(Continued)

Page

Table of Contents
(Continued)

Page

Volume III

Table of Contents
(Continued)

Page

Table of Contents
(Continued)

Page

Volume IV

Table of Contents
(Continued)

Page

Table of Contents
(Continued)

Page

Volume V

Volume VI

Table of Contents
(Continued)

Page

Table of Contents
(Continued)

Page

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA,

v. 14 Cr. 68 (KBF)

ROSS WILLIAM ULBRICHT,

Defendant.

----------x

New York, N.Y.
January 29, 2015
9:10 a.m.

Before:

HON. KATHERINE B. FORREST,

District Judge

APPEARANCES

PREET BHARARA,
United States Attorney for the
Southern District of New York
BY: SERRIN A. TURNER
TIMOTHY HOWARD
Assistant United States Attorneys

JOSHUA LEWIS DRATEL
LINDSAY LEWIS
JOSHUA HOROWITZ
Attorneys for Defendant

- also present -

Special Agent Vincent D'Agostino
Molly Rosen, Government Paralegal
Nicholas Evert, Government Paralegal

A. I would say hundreds of bitcoin transactions.
Q. Including the bitcoin transactions you talked about earlier, you seized bitcoins?
A. Correct, for the government seizure of bitcoins as well.
Q. What are bitcoins?
A. Bitcoins are -- it's digital currency. It's money that works online to buy products online or even in real person or paid-for services. It's kind of like cash for the Internet. It's similar to cash in that when people conduct transactions, you don't really see who is doing the transactions, but it's different than cash that every single transaction, the transaction itself, it gets permanently documented on this thing called the block chain. So even though you don't know who made the transactions, you get to see every single transaction that was performed using bitcoins.
Q. Can you explain the block chain a little more fully, please.
A. So block chain, in accounting terms it's similar to a public ledger which means, you know, published financial records of everything that's taking place. So block chain, it's a file that's online on the Internet access and shared and used by all the bitcoin users and what it contains is every single transaction of bitcoins ever since the creation of bitcoins.
Q. Now, can bitcoins be used for legitimate purposes?

A. Yes, they can.

Q. Can they also be used for illegitimate purposes?

A. Of course.

THE COURT: Let me ask about the block chain again.

I'm not clear what information is in the block chain. In other words, I understand from your testimony that you can follow that there has been a transaction, then another transaction, then another transaction and you can follow the transaction history of a particular bitcoin --

THE WITNESS: Right.

THE COURT: -- or a portion of bitcoin.

THE WITNESS: Yes.

THE COURT: What is the information in the block chain?

THE WITNESS: So the information that's contained in the block chain, first of all, you would have the information about the block chain itself, so the size of the current block and the date and the time that block was added to the block chain, so it's constantly growing. I think the current size of the block chain is over 20 gigabytes I think. So it's a considerable size because it contains all the history of bitcoins.

So within the block, there's additional information of every single transaction that was added to that block, so you'll see all the addresses that were used to send the payment

and all the addresses that were used to receive a payment in bitcoins.

THE COURT: IP addresses?

THE WITNESS: There is no direct IP address of who is sending and receiving bitcoins.

THE COURT: So what kind of address is it?

THE WITNESS: I believe you might be able to obtain the IP address of --

THE COURT: Don't speculate. I'm wondering when you use the word "address," what were you referring to, what kind of address.

THE WITNESS: Bitcoin addresses. So it's a long string of alphanumeric value and it works almost like an email address. You need to give somebody your bitcoin address in order for whoever that wants to pay you to make sure they pay you the correct amount of bitcoins to the right person.

So if I were to email Tim, I wouldn't know how to send him an email until Tim gave me his email address. So in the same manner, if I need to send Tim ten bitcoins, there's no way for me to deliver those bitcoins to him unless he gives me his bitcoin address first.

BY MR. HOWARD:

Q. Mr. Yum, let's skip ahead. We'll come back to where we want to go next to show an example of a block chain. Look at Government Exhibit 601, which is in your binder, please.

Do you recognize what this is?
A. Yes, I do.
Q. What is this?
A. It's a screenshot of a popular block chain explorer, blockchain.info. You could obtain information about the block chain and transactions.
Q. Is that website available to the public?
A. Yes.
Q. Were you involved in the preparation of this exhibit?
A. Yes.
Q. Does this exhibit fairly and accurately depict information from the block chain?
A. Yes, it does.
MR. HOWARD: Government offers Government Exhibit 601.
MR. DRATEL: No objection.
THE COURT: Received.
(Government's Exhibit 601 received in evidence)
Q. Mr. Yum, this is something you could pull up in an ordinary Internet processor, correct?
A. Yes.
Q. Let's focus on the top section.
A. So the top section is a high-level summary about that address.
Q. So where is -- do you have your laser pointer up there?
A. Yes, I do.

of the information about her bitcoins.
Q. What else does having the private keys allow you to do with bitcoins?
A. So if you own any bitcoins in any one of these addresses, the corresponding key allows you to spend those bitcoins.
Q. And the wallet is basically just a computer file, correct?
A. Yes. It's a computer file, yeah.
Q. Is Alice able to see all of her own addresses?
A. Yes.
Q. Just to be clear, on this demonstrative that we say BTC Address 1 and down to 5.

How many addresses could a wallet contain?

A. As many as you want. In here for example purposes there's only five addresses listed, but you could create hundreds, thousands of addresses in one wallet file.
Q. Can anyone else other than Alice see all of the addresses in her wallet?
A. Only if they know what the address is, but if you don't have the private key, you can't just guess someone else's address.
Q. To be clear, each those addresses is one of those long, ugly string of numbers and letters, right?
A. Correct.

THE COURT: Where do you get an address?

THE WITNESS: So, the bitcoin program generates a long

string of numbers and that acts as a seed to the private key. And the program again uses that private key to calculate something that is similar to the MD5 hashes and a hash value is represented as a public key which is a lot easier to pass to someone else, although it looks very long and confusing.

THE COURT: All right.

Q. How easy is it to create a new bitcoin address?

A. If you're using a bitcoin program all you have to do is click a button and request the program to create a new bitcoin address.

Q. It will assign a new bitcoin address to you?

A. Yes.

Q. Will it give you the private key necessary to spend the bitcoins in that address?

A. Right. In the background of the program, you'll get a private key and then you'll get the public address that you can freely give out to other people if you want to receive bitcoins to that address.

Q. Could you explain what is depicted on the second slide, please.

A. I'm going to walk you through a simplified demonstration of how a transaction would occur. So, again Alice, she owes Bob ten bitcoins, but just as I said, Alice has no idea where to send the bitcoins to, so she needs to ask Bob for a bitcoin address first.

So Alice wants to send ten bitcoins and she's asking where to send it to. And Bob, in his wallet, he only has two addresses, but as stated before, he could have many more if he wants to. So Bob picks his Bitcoin Address 2, and can we go to the next screen, please, and tells Alice to send ten bitcoins to Address 2.

Alice doesn't really need to worry about where the bitcoins are coming from her wallet. The program handles that in the most efficient manner it could, so once Alice tells her bitcoin program to send ten bitcoins to Bob's Address 2, Alice's program picks Address 1 and Address 4 in her wallet and sends ten bitcoins to Bob's Address 2.

Q. So Alice doesn't have to pick and choose between her own addresses, correct?

A. Right. It's very simple to use.

THE COURT: It could be five out of one address, five out of another or two out of one address, eight out of another, or some other combination of pieces?

THE WITNESS: Correct.

THE COURT: All right.

Q. So what's depicted on the third slide?

A. In our demonstration, there were seven bitcoins in Address 1 that was sent and three bitcoins in Address 4 of Alice's bitcoin that were sent to Bob's Address 2 in the amount of ten bitcoins.

Q. And then what's reflected on the bottom of the slide?
A. So the bottom would be an example of what would be recorded onto the block chain as we saw in the prior block chain info screenshot. So in here, you would see a unique transaction number that identifies this particular transaction and the date and time this transaction was documented onto the block chain.

And in here, again, you see only the two addresses that were used to make this transaction of ten bitcoins that were sent to Bob's Address 2.

Q. So now Bob could get this information off the block chain and see what addresses Alice's wallet used to engage in this transaction, correct?
A. Correct. Bob, he knows his address, so he could easily search his own address and figure out this transaction and note that Alice used these two bitcoin addresses to send Bob ten bitcoins.
Q. Now, would Bob know all of Alice's other bitcoin addresses?
A. No. Address 2, 3 or 5, Bob would have no idea what the -- who those addresses belong to.
Q. And why couldn't he see those?
A. The addresses aren't announced or anything. So unless you directly have a transaction with somebody, you can't really figure out who owns what address.
Q. You need the private keys to see all the rest of the wallet?

A. Right. The only way Bob may be able to see these addresses is if he had the private key in his wallet allowing him to calculate the same private address -- public address.

Q. Now, Mr. Yum, earlier you testified that you seized approximately 20,000 bitcoins from the Iceland bitcoin server, correct?

A. Correct.

Q. Now, apart from that seizure, were you involved in any other seizures of bitcoins in the Silk Road investigation?

A. Yes, I was.

Q. Where were those bitcoins located?

A. The wallet file for the other bitcoins were obtained from the laptop that was seized from the defendant on the day of his arrest.

Q. And how did you get access to that wallet file?

A. So, Mr. Kiernan actually analyzed and reviewed the laptop and he had located the wallet file and copied it onto a thumb drive and handed it over to me.

Q. And what did you do with that wallet file after it was provided to you by Mr. Kiernan?

A. So, I loaded that wallet file onto my bitcoin program instance, and checked the current balance that was contained inside all the addresses inside the wallet file.

Q. And what was the balance?

A. It was approximately 144,000 bitcoins.

Q. And what were those bitcoins worth approximately at the time of the defendant's arrest?
A. So at the time of the arrest, which was prior to when I received that wallet file, it was -- again, using the varying bitcoin price of that day, it would have been anywhere between 16- to $18 million.
Q. Now, what did you do after you determined the balance of the bitcoins that were in the wallet that was in the defendant's computer?
A. I had another bitcoin address that was prepared for the government's seizure, and I transferred all the bitcoins from the defendant's wallet file into the government address.
Q. You said it was an FBI bitcoin wallet, correct?
A. Correct.
Q. Is this the same or different wallet that you used in Iceland to get the bitcoins from the bitcoin server?
A. Different address. I wanted to separate the two so the bitcoins didn't mix.
Q. Was there any balance in the FBI controlled log when you created it?
A. No. It was a newly -- brand new created bitcoin address and since it's never been -- there's never been a transaction conducted using that address, it wouldn't have shown in the block chain, so no one else knew what that address was.
Q. Now, did the wallet file that was provided to you by

Mr. Kiernan from the defendant's laptop contain the private keys for the bitcoin addresses in that wallet?

A. Correct. That would be the most important thing. Without those private keys, I wouldn't have the right to send the bitcoins from the defendant's wallet to the government seizure address.

Q. Did those private keys also allow you to see all of the bitcoin addresses that were located in that wallet?

A. Yes.

Q. Can you please flip in your binder to what's been marked for identification purposes as Government Exhibit 607. Do you recognize what this is?

A. Yes, I do.

Q. And what is this?

A. It's a screenshot of a search engine named duckduckgo, and it's the search result for a bitcoin address starting 1FfmbH, which is the address that I created for the government to seize all of the bitcoins from the defendant's laptop.

Q. And had you previously used this website to obtain public information from the block chain?

A. Yes, I have.

Q. Does this website accurately reflect bitcoin transactions that you've conducted in the past?

A. Yes, it does.

Q. You took this screenshot?

A. Yes.

MR. HOWARD: The government offers Government Exhibit 607.

MR. DRATEL: No objection.

THE COURT: Received.

(Government's Exhibit 607 received in evidence)

Q. Mr. Yum, right up here at the top next to the cute little picture of the duck, there's 1Ff and a long string of characters. What is this?

A. That's the address created for the government.

Q. The bitcoin address?

A. The bitcoin address, yes.

Q. And you were involved in creating that, correct?

A. Yes.

MR. HOWARD: Can we zoom out, please.

Q. Here it says total received, 144,341 and change. What does that number represent?

A. So that's the total amount of bitcoins that was sent to this address above.

Q. And where were they sent from?

A. So that total number is a little higher than the actual amount, but the majority of those were sent from the defendant's laptop -- the wallet file located in the defendant's laptop.

MR. HOWARD: Mr. Evert, could you please publish

Government Exhibit 201L, which is already in evidence.

Q. Have you seen this before? It's on the screen.

A. Yes, I have.

Q. And what is this?

A. It's a summary sheet. It's a picture screenshot of the defendant's laptop when it was seized on the day of his arrest.

Q. So I want to focus here on the fifth line down here. Can we zoom in here. And here it says cold BTC and under that 144,336.4.

How does this number that was on the defendant's computer screen compare to the number of bitcoins that you seized?

A. It matches almost exact to the amount that was seized.

Q. And right above that, there's the word "cold BTC"?

A. Yes.

Q. Are you familiar with the bitcoin term "cold storage"?

A. Yes, I am. It's a term that's commonly used within the bitcoin community and bitcoin users.

Q. What is it used to refer to?

A. It's a way to store your wallet file. So it's important to secure your wallet file because it has all the keys that allows you to spend your bitcoins. So cold storage is -- the most common example is not having your wallet file attached a bitcoin program. So instead of -- that would be hot, so instead of having a hot wallet, you have a cold storage where

Q. Those are two servers that you were actually personally involved in seizing, correct?
A. Yes, when I was still with the government.
Q. Did you find the private keys on those servers for those wallet files?
A. Yes. So I obtained the wallet files, so I had all the private keys that are also inside those wallet files.
Q. So did that allow you to see all of the bitcoin addresses that were associated with those wallets on the Silk Road servers?
A. Yes.
Q. Now, how about the defendant's laptop?
A. So, I took the same approach. I got a forensic image copy of the defendant's laptop and I examined and analyzed the laptop to locate at least three wallet files and extracted all the bitcoin addresses there because I had the private keys that were contained inside those wallet files.

(Continued on next page)

Q. Now, you testified that you examined -- you received certain pieces of evidence from the FBI to perform this analysis, correct?
A. Correct.
Q. So what pieces of evidence did you specifically receive?
A. I got three forensic images -- one of the Philadelphia server, the backup server, one of the Iceland bitcoin server that was seized over in Iceland, and an image of the defendant's laptop, which was seized at the time of his arrest.
Q. So if you could please flip in your binder -- actually, just real fast. After you received copies of those three pieces of evidence, did you do anything to verify that they were true and accurate copies of the original evidence?
A. Of course. I calculated my own MD5 and SHA1 hashes. I calculated those two hash files to make sure my starting point is the same as what was originally copied.
Q. So did you compare those MD5 and SHA1 hash values to the ones that were originally generated for those pieces of evidence?
A. Yes.
Q. What did you discovery?
A. They all matched.
Q. Could you please flip in your binder to what has been marked as Government Exhibit 606, please.
How many pages is this exhibit?

A. Three pages in total.
Q. And what is it?
A. Each one of those pages are a screenshot that I made after I calculated the hash values.
Q. Those are the hash values of each of the three pieces of evidence that you received from the FBI?
A. Correct.
MR. HOWARD: The government offers Government Exhibit 606.
MR. DRATEL: No objection.
THE COURT: Received.
(Government's Exhibit 606 received in evidence)
Q. So each contains an MD5 and a SHA1, correct?
A. Correct.
MR. HOWARD: Just flip through the pages, Mr. Evert.
Q. And all of those values match the values on the various log files we've seen today, correct?
A. Yes, they do.
Q. And also match the log file from the image of the defendant's computer that you received from the FBI?
A. Yes.
Q. The laptop computer?
A. Yes.
Q. Could you please look in your binder to what has been marked for identification purposes as Government Exhibit 609.

Do you recognize this exhibit?
A. Yes, I do.
Q. And what is it?
A. It's a simplified illustration of the work that I did to compare all the addresses that was obtained from Silk Road Marketplace and all the addresses that were obtained from the defendant's laptop.
Q. And would this aid your testimony today?
A. Yes.
MR. HOWARD: The government offers Government Exhibit 609 for demonstrative purposes.
MR. DRATEL: No objection for demonstrative purposes.
THE COURT: 609 is received for demonstrative purposes.
(Government's Exhibit 609 received in evidence)
BY MR. HOWARD:
Q. Could you please explain what your analysis consisted of?
A. Sure. So I examined the forensic copy of the defendant's laptop and carefully went through the files and located three Bitcoin Wallet files. Some of those wallet files may be duplicates or used that one time and then switched over to a different wallet, so there were some duplicates. But at the end I sorted the addresses down to 11,135 unique individual bitcoin addresses.
And this is possible because the wallet file contains

the private key that I was talking about. So without the private key I would not be able to extract all these addresses.
Q. The fact that the private keys were located on the defendant's computer, what does that indicate?
A. It indicates the defendant's laptop, the wallet file, controlled these bitcoin addresses. So these are the only keys that could spend the bitcoins that are in these wallet files.
Q. So the user of the computer could spend the bitcoins in those addresses?
A. Correct. And if we could go to the next page.

So from the other side, those are the two servers -- images of two servers that I obtained, one from the Philadelphia backup server and one from the Iceland Silk Road bitcoin servers. So from those two images, I carefully went through them, examined it, and identified and located 22 Bitcoin Wallet files. Again, some of these might be backups or an address that was used at one point and moved on to another address. So initially I found over 10 million bitcoin addresses. Some of them are duplicates, but I narrowed it down to a little over 2 million unique bitcoin addresses.
Q. Go to the next page, please.
A. So now I have two sets of addresses, a set of over 2 million bitcoins that were found on servers that are related to Silk Road Marketplace. And on the other side I had over 11,000 bitcoin addresses that were recovered from the laptop belonging

to the defendant that was seized at the time of the arrest.

Q. Sorry, how many address? 2,105,527 unique addresses?

A. Yes. The exact number would be 2,105,527 addresses from Silk Road Marketplace and 11,135 bitcoin addresses from the defendant's laptop.

Q. Go to the next page, please.

A. Wait. Actually, can we go back one?

So I could explain using this screen and the next screen, but the analysis that I did, I didn't do any complicated analysis. I wanted to look for the most simple direct link between those two sets of addresses. So I had the addresses from the Silk Road Marketplace and I had the addresses from the defendant's laptop, and I went back to the block chain, which is publicly available and agreed by all the bitcoin users, and identified all the transactions where the money was being sent from Silk Road Marketplace and bitcoins were received to the addresses on the defendant's laptop.

Q. Are these direct one-to-one transactions?

A. Direct one-to-one. It didn't skip over anywhere else. It went straight directly from Silk Road Marketplace directly to the addresses found on the defendant's laptop.

So if you could go to the next screen.

So just to give you an example of the raw information that I had to work with, this is not the entire list but just a portion of addresses from each side. So on the left you see

all the addresses, the public addresses for Silk Road Marketplace, and the unique list had over 2 million bitcoin addresses and I could obtain these because of the private key that was also inside the wallet files.

On the right side you have the laptop addresses in there. These are the unique addresses, over 11,000 bitcoin addresses that were found on the defendant's laptop and. I was able to tell these because the wallet file contains the private keys to generate these public addresses, which also allows the owner of those private keys to spend those bitcoins.

MR. HOWARD: Your Honor, may I approach?

THE COURT: Yes.

Q. So I'm handing you what has been marked for identification purposes as Government Exhibits 650 and 651.

Do you recognize what these are?

A. Yes, I do.

Q. And what are they?

A. Each one of theses discs contain the text file that you saw a portion of just now.

Q. What are in those text files?

A. One of the text files contains all the addresses -- all the unique list of addresses from the Silk Road Marketplace, and the other disc contains all the unique addresses found on the defendant's laptop.

Q. And just to be clear: I gave you two CDs. Which one is

which?

A. Exhibit 650 is the Silk Road Marketplace bitcoins, and Exhibit 651 is all the addresses that were found on the defendant's laptop.

Q. And how do you recognize these CDs?

A. I was involved in the creation of these CDs.

Q. And are your initials on them?

A. Yes. After I created them, I initialed them and dated the CDs.

MR. HOWARD: The government offers Government Exhibits 650 and 651.

MR. DRATEL: No objection.

THE COURT: Received.

(Government's Exhibits 650 and 651 received in evidence)

MR. HOWARD: Your Honor, may I approach?

THE COURT: You may.

MR. HOWARD: So, Mr. Evert, could you please publish Government Exhibit 650. Just bring it up in the text file itself.

Q. So, Mr. Yum, this the list of the two-million-plus unique bitcoin addresses that were recovered from Silk Road-related servers, correct?

A. Correct.

MR. HOWARD: If you can scroll this to show how large

MR. HOWARD: Could you please publish Government Exhibit 610.

Q. So, Mr. Yum, can you please walk us through what this shows?

A. Sure. I guess it is best to start from the middle. So that section is, as you've seen before from the example of blockchain.info, the website where you can look up all the bitcoin transactions, this is a transaction that I identified which had bitcoin addresses from the marketplace making 3,900 bitcoin transactions to a bitcoin address that was found on the defendant's laptop.

So that's the unique transaction ID. It was -- the transaction was made April 3rd, 2013. Again, you see the address starting on 1GarVY. And up top it has a screen capture of the list of the addresses from the marketplace that you had seen previously and a location where that can be found in that list.

On the bottom this has the portion of the list of all the addresses from the defendant's laptop, and you could see that the address found in there, starting "17t6V," matches the received bitcoin address in this transaction.

Q. So this exhibit shows 3,900 bitcoins were sent from an address that was located on Silk Road servers to a bitcoin address that was located on the defendant's laptop?

A. Yes. Exactly.

Q. And that happened on April 3rd, 2013, according to publicly available information on the block chain?
A. Yes.
Q. Now, was this the only transaction that you found linking the bitcoin addresses on the Silk Road servers to the defendant's -- the addresses on the defendant's laptop, or were there others?
A. No. There were almost 4,000 unique transactions from Silk Road Marketplace to the addresses that were found on the defendant's laptop.
Q. So could you please flip in your binder to what's been marked for identification purposes as Government Exhibit 620.
Do you recognize this exhibit?
A. Yes, I do.
Q. And what is this exhibit?
A. This is a list of all the transactions that I was successfully able to identify.
Q. Did you participate in the creation of this exhibit?
A. Yes.
Q. Does this exhibit accurately summarize information from the bitcoin addresses that you found -- that you reviewed from wallets found on the Silk Road servers and the defendant's computer?
A. Yes.
Q. Does this exhibit accurately summarize information that you

retrieved from the block chain regarding bitcoin transactions?
A. Yes.
MR. HOWARD: The government offers Government Exhibit 620.
MR. DRATEL: Objection, your Honor. *Crawford*, foundation, hearsay.
THE COURT: All right. Those objections are overruled. Government Exhibit 620 is received.
(Government's Exhibit 620 received in evidence)
BY MR. HOWARD:
Q. So, Mr. Yum, what was the date range of the transactions that you located?
A. The first transaction occurred in September 24th, 2012, and the latest transaction I was able to identify was August 21st, 2013.
Q. And were the transactions spread across -- the thousands of transactions were spread across that time period?
A. Right. It was spread across almost all of that entire one-year span.
MR. HOWARD: So, Mr. Evert, could you just go to the top, please. Just zoom in on the first few rows.
Q. Could you just describe what is depicted here?
A. So it is a simplified version of all the screenshots that you saw before, prior. So that's -- the first column is there is the time stamp, the time that this transaction was included

onto the block chain. The second column there is the unique transaction ID that you could locate, pinpoint to the exact transaction that's happened. So behind those transactions you would actually see the addresses that are used to send bitcoins to another receiving address, but you could easily also refer to those two transactions by that transaction ID.

And the last column there, that's all the bitcoins that were involved in that transaction that ended up in the wallets found on bitcoin addresses found on the defendant's laptop.

Q. So to be clear, Mr. Yum, you could put that unique transaction number into the block chain on the website to get the addresses that were involved in the transaction?

A. Correct.

Q. And those addresses matched the addresses that you found on the Silk Road servers and the defendant's laptop?

A. Yes.

MR. HOWARD: Can we just scroll to the bottom of the chart.

(Indicating)

MR. HOWARD: This is page 64 of the exhibit. Could you zoom in on the bottom.

Q. And so the total was 700,253.91 bitcoins, is that correct?

A. That's correct.

Q. Now, Mr. Yum, can you please flip in your binder to what's

been marked for identification purposes as Government Exhibit 620C.

What is this?

A. It appears to be a price index from a website coindesk.com. It shows the date and the closing price of the bitcoins in U.S. dollar amount.

Q. According to coindesk?

A. According to coindesk.

Q. Is that information available on a public website?

A. Yes.

Q. Now, is coindesk widely recognized and used by the bitcoin community for bitcoin pricing?

A. Yes, not only bitcoin pricing but other data and news and information about bitcoins.

Q. Now, based on your knowledge of the bitcoin community, would you agree that the reputation of coindesk carries some weight and is recognized as accurate in the community?

A. Yes.

Q. Does this exhibit accurately summarize pricing information for bitcoins from coindesk?

A. Yes, it does.

MR. HOWARD: The government offers Government Exhibit 620C.

MR. DRATEL: No objection.

THE COURT: Received.

(Government's Exhibit 620C received in evidence)

THE COURT: We're going to -- Mr. Howard, in about three minutes we are going to break for lunch.

Q. Can you just briefly explain what is depicted here?

A. So on the left column it has the date of these records. On the right column it has the end-of-the-day closing price of bitcoins, represented in U.S. dollar amounts, for each corresponding date.

Q. Now, could you please flip in your binder to what's been marked for identification purposes as Government Exhibit 620A.

What is this exhibit?

A. It is a summary spreadsheet of the analysis that I conducted.

Q. Did you participate in the creation of this exhibit?

A. Yes.

Q. Does the exhibit accurately summarize information from the bitcoin addresses you reviewed from bitcoin wallets found on the Silk Road servers and on the defendant's computer?

A. Yes, it does.

Q. Does the exhibit accurately summarize information from the block chain regarding bitcoin transactions?

A. Yes.

MR. HOWARD: The government offers Government Exhibit 620A.

MR. DRATEL: Objection. The same grounds, your Honor.

Hearsay, foundation --

THE COURT: All right. Those objections are overruled. Government Exhibit 620A is received.

(Government's Exhibit 620A received in evidence)

MR. HOWARD: Can we zoom in on the top, please.

Q. Mr. Yum, could you please describe what's depicted in this chart?

A. Yes. So it's a monthly summary breakdown of all the transactions that took place between addresses found on Silk Road Marketplace sending bitcoins to the addresses found on the defendant's laptop.

So the span, again, starts from September 2012 all the way down to August 2013. And for each month the second column shows you the number of transactions that were conducted. The third column shows you how many bitcoins in those transactions were sent from Silk Road Marketplace to the addresses found on the defendant's laptop. And the last column is the, I guess, realtime conversion of U.S. dollar amounts for each one of those dates where the transactions were identified.

Q. And did you use the coindesk information to convert to U.S. dollars?

A. Yes.

Q. What do you mean by "realtime" conversion?

A. So I didn't just take one day, let's say -- you were asking me before how much bitcoins were at the time of the arrest. I

didn't use one dollar amount. From the prior exhibit, I took each individual day's closing and matched it to each of the individual day's transactions and correctly calculated how much bitcoins were worth at the time of that transaction.

Q. So this exhibit reflects that there was a total of $13 million worth of transactions at the time that each transaction took place?

A. Yes.

Q. And a total of 700,254 bitcoins received --

A. Correct.

Q. -- from Silk Road servers to the defendant's laptop wallets?

A. Yes.

Q. And 3,760 transactions, correct?

A. Correct.

Q. Could you please take a look at 620B in your binder.

Do you recognize what this is.

A. Yes, I do.

Q. And what is this?

A. It's a pie chart that I created also summarizing an analysis that I did.

Q. Did you participate in the creation of this exhibit?

A. Yes, I did.

Q. Does this exhibit accurately summarize information from the bitcoin addresses you reviewed from wallets found on the Silk

Road servers and the defendant's computer?

A. Yes.

Q. And does it accurately summarize information from the block chain regarding bitcoin transactions?

A. Yes.

MR. HOWARD: The government offers Government Exhibit 620B.

MR. DRATEL: The same objections, your Honor.

THE COURT: All right. Those objections are overruled. 620B is received.

(Government's Exhibit 620B received in evidence)

Q. Mr. Yum, could you please explain what is depicted here?

A. So you see a pie chart in there, and the biggest, red part has the 700,254 bitcoins that I correctly identified coming from Silk Road Marketplace and being transferred to the addresses found on the defendant's laptop.

I didn't stop there. I went back and analyzed all the addresses on the defendant's laptop. And I've also found 89,000 other bitcoins that were sent to the addresses that were found on the defendant's laptop.

So to, I guess, give you a summary of what I just said, the defendant's -- addresses found on the defendant's laptop received a total of almost 790,000 bitcoins, and out of that 88 -- almost 89 percent were bitcoins that were transferred from the Silk Road Marketplace directly to the

defendant's laptop in the amount of 700,254 bitcoins.

Q. When you say "directly," you mean one-to-one transfers, correct?

A. One-to-one transfers.

So that 89,854, it could have came from other sources but it could have also --

MR. DRATEL: Objection.

THE COURT: Sustained.

MR. HOWARD: This might be a natural breaking point, your Honor.

THE COURT: All right. Ladies and gentlemen, we're going to take our lunch break now and come back at 2 o'clock.

I want to remind you all not to talk to each other or anybody else about this case. And, also, if you see any news articles about this case, you are to not read those news articles. Turn away your eyes. All right? I instruct you to do so.

Thank you. We'll see you after lunch.

THE CLERK: All rise as the jury leaves.

(Continued on next page)

(Jury not present)

THE COURT: You may step down. Have lunch until 2 o'clock. I will see you back on the stand at 2.

(Witness not present)

THE COURT: All right, ladies and gentlemen. Let's all be seated.

I wanted to make certain that we addressed the two exhibits and I have one other matter and then whatever else you folks would like to address before we break for lunch ourselves.

There were objections by Mr. Dratel to Government Exhibits 620 and 620A on *Crawford*, which I take it, Mr. Dratel, was because of an argument that we discussed yesterday afternoon of insufficient notice?

MR. DRATEL: No. It is really about the underlying -- in other words, you have a couple of preliminary steps in Mr. Yum's analysis. Then you have an intermediate step and then you have a final step, and we don't know how we get from the intermediate step to the final step.

THE COURT: You can take him through that on cross-examination.

MR. DRATEL: I understand. But there is no foundation for it, and I believe that it is probably something that creates a *Crawford* confrontation issue, similar to other sort of scientific or computerized issues, where something is done

and then someone comes in and presents something that is essentially the work of a computer program and it is not -- you know, it hasn't been verified. You know, I don't know what his relationship is with the program. We don't know any of that. We don't have any underlying stuff as to how it was done. It is not a simple process, and I don't think it was done manually.

THE COURT: Was that the nature of your *Crawford* objection both for 620 and 620A?

MR. DRATEL: Yes, your Honor.

THE COURT: All right. So at this point I don't find there to be any traction to that objection and so it was overruled before. If after cross-examination you have some basis to renew the application, then you can go ahead and do so. See what you want, what you can develop on cross-examination. You are certainly entitled to go into all aspects of how he performed this exercise.

MR. DRATEL: And with respect to the notice, your Honor, my application would be, again, to put off the cross until Monday morning so that we can absorb stuff that we were actually hearing for the first time about a document that has, as you can see now, an extraordinary number of transactions. There is zero backup. Zero anything for it. We have been trying to develop what we can but we still need more time to do that.

THE COURT: When you say that there is zero backup, zero anything, my understanding from our conversation yesterday afternoon was that all of this information, which is the very information at the heart of this case, was produced during discovery.

Mr. Howard.

MR. HOWARD: That's correct. On Sunday night we provided the spreadsheets --

THE COURT: Let's go back first to what was --

MR. DRATEL: The analysis, how the analysis was done.

THE COURT: Mr. Dratel, let me just make sure I have got the facts in order.

Tell me when and what was produced that underlies this analysis during the discovery.

MR. HOWARD: Yes. For almost a year now, the defendant has had access to images of his laptop and the various servers where these log files were contained, including what's been referred to as the Philadelphia backup server and the Iceland bitcoin server. Those images included all of these bitcoin wallets and the private keys for those wallets, which is the same images the witness just talked about. Based on that, all of this information, all of the bitcoin addresses were stored in those wallet files that have been available to the defendant for over a year.

THE COURT: All right. And then, as I understand it

from our conversation just before we all adjourned last night, the analysis that is at 620 and the summary of that, where the comparison was done, that analysis was performed during the course of this trial and was produced on Sunday; is that right?

MR. HOWARD: Yes, you are right, your Honor. And within a couple of hours of actually us receiving the spreadsheets that had all the data in them and, you know, the much more complicated and much more voluminous than the summary charts that we're pushing into evidence, but that was produced promptly to the defense as soon as we had them generated.

THE COURT: All right. Mr. Dratel.

MR. DRATEL: A couple of things. One is they had it, too. So why are we getting this in week three of trial if they had all of this information before as well? Why did they prepare this analysis -- they've only started once the trial started.

THE COURT: Well, as I understand it, this all went back to your opening statement.

MR. DRATEL: Yes. But what I'm saying is to say that we had all the wallets and the addresses is immaterial in the sense that they had it too. If they wanted to put together an exhibit that linked all of that, they should have done it in advance of trial, not -- and they've done it during trial, OK, but I should have the opportunity -- this witness, it took more than a hundred hours to prepare this analysis. I've had it for

maybe 80, not including the time in court and sleeping and doing all the other stuff that needs to be done in this case. So it's really no time at all. This witness took a hundred hours. They got paid $55,000 for this.

THE COURT: Well, the objections are overruled, as I've said. And in terms of timing, we will go into cross-examination right after the government is done with its direct examination with this witness.

The materials that underlie the analysis were produced long ago. Based upon the opening statement and based upon one of the theories of the defense, which is that the defendant was a bitcoin trader and that any bitcoins in his possession were from bitcoin trading, it was reasonable to expect that you yourself had done such an analysis and, therefore, that you had some intention of presenting something that would have shown the opposite. In any event, you've opened the door to it, and we're going to proceed. And the fact that the government adjusted and was able to do so is not something that is particularly problematic or unusual. So that's my ruling on that.

So we'll proceed with cross-examination with this witness after lunch.

MR. DRATEL: Your Honor, what I'm asking for, in functional terms, is a two-and-a-half hour accommodation so that I can prepare a proper cross-examination of this witness.

THE COURT: I have heard your application, and we're going to go directly into the cross-examination of this witness. If you --

MR. DRATEL: Then I am making a notice objection to the entirety of that level of his testimony --

THE COURT: The objection is overruled. I think you've got your position well and truly stated on the record. If you have any additional positions you want to state, you can file it in a letter on the docket.

In terms of hearsay, there is no hearsay issue with these documents, and certainly the foundation was well established for these. So those objections are similarly overruled.

Mr. Howard, would you like to address or fill out the record in any regard yourself?

MR. HOWARD: Yes, your Honor.

The fact is, as you correctly stated, this door was opened by the defense during their opening statement. They made a claim about the source of the bitcoins that were recovered from the defendant's wallet files. In response to that, we performed an analysis with the help of outside consultants. As soon as that analysis was ready, we produced the underlying data to the defense. We produced some summary charts today in court.

It should be noted that there was some time that was

Q. Who was that?
A. It's a colleague of mine.
Q. And what is his name?
A. Mathew Edmond.
Q. And what's his -- what are his credentials?
A. He has a doctorate in cryptology.
Q. What did he do as part of this project?
A. He worked with me to identify the wallets, extract the bitcoin addresses, and compare that to the block chain.
Q. Did he do that actual work?
A. We both did.
Q. So he did some of that work?
A. Yes.
Q. Correct?
How many hours did he put into that?
A. We both worked on it for about a week together, so I think we're a little short of 100 hours. He put in about 60. I put in about 40.
Q. And what were his contributions to Government Exhibit 620 which is the spreadsheet, the large spreadsheet with all of the transactions. Right, isn't that the --
A. Yes.
Q. So what's his contribution to that?
A. He assisted me in obtaining the underlying raw information for that summary.

Q. And how was that exhibit created?
A. That one? I believe I just summarized the Excel file, so that's an Excel spreadsheet. I took all of the raw data and created a summary chart on Excel.
Q. But in terms of the matching, did you use any software to match the transactions?
A. Oh, the actual analysis?
Q. Yes.
A. Yeah, we loaded all the information onto a table and did a query on that table to find the matching transactions.
Q. And what program?
A. I believe the actual matching was done through Python.
Q. And what is Python?
A. Python. It's a scripting language.
Q. Did you have any participation in writing the code for that program?
A. Actual hands-on typing was done by Mr. Edmond, but we both sat down to work out the logic.
Q. But I mean in terms of the program itself, did you create that program?
A. Oh, no. So the reason why we use Python is there's available software called Pie Wallet, which was also found on the defendant's laptop, it's a common Python application that's used to manage bitcoins. So we used commands that are commonly used by all the bitcoin users.

Q. I'm not talking about keys. I'm talking about bitcoins themselves.

Bitcoins themselves, the wallets -- the addresses within the wallets that the bitcoin were in, they were basically in one wallet, correct?

A. The majority came from one wallet.

Q. Right. And that wallet had a bitcoin program running in it, right?

A. Yes, but the program hasn't run since August of 2013, so -- it will be a cold wallet at that point.

Q. But isn't a cold wallet where it's not connected to a program where you can actually take the wallet, put it in a file or in a folder or somewhere else on the computer and extract the program -- extract it from the program so that it can't execute any functions, right?

A. Well, a cold wallet is something that's not online. So if the wallet's last access date was August 2013, it hasn't been online since August 2013; therefore, from August until October, it's a cold wallet because it never went online.

Q. But it still has a program in it, right, and it's still capable of execution?

A. Right, but it didn't execute because it would have updated that last-access date on the wallet.

Q. But if someone doesn't use their wallet, it doesn't mean it's a cold wallet; it can still be a hot wallet. You're just

not using it, right?
A. No, not correct.
MR. TURNER: Objection; asked and answered.
THE COURT: I'll allow it.
A. A hot wallet is a wallet that is currently connected to the Internet.
Q. At that time? At the very time?
A. At the very time.
Q. That's your definition?
A. Yes, it is.
Q. Okay. And how many bitcoin cases did you have before this one?
A. This was a second case I believe.
Q. Now, you talked about identifying servers and identifying bitcoin server, right, and identifying the servers from the Philadelphia servers, right?
A. Right.
Q. You testified about that. What you saw from the code was only an onion address, right? In other words, looking back to find the servers, correct, it wasn't an IP address. It was --
A. I'm sorry. Which address and which server are you referring to?
Q. The server to which the backup data was exported to the jtan -- the Philadelphia server, right?
A. Correct.

Q. From the Iceland server, right?
A. Yes.
Q. Now, what you saw there when you're looking to find that is an onion address, right, an onion url, dot-onion url, correct?
A. I was brought onto the case around that time, and I received an IP address. And my -- the investigative team, before I joined, they were the ones who did the analysis, so I can't speak to what allowed me to receive that IP address, but I received that IP address. Nothing else.
Q. Now, the servers were first -- you went in October to Iceland, correct?
A. Correct.
Q. And to be there at the time of the arrest to shut down the servers, correct?
A. Yes.
Q. And to put the seizure banner up, we saw at Exhibit 600, right?
A. Right.
Q. The government had access to the servers -- the U.S. government had access to the servers in July of 2013, correct?
A. That's what I've been told --
MR. TURNER: Objection; foundation.
THE COURT: Sustained.
Q. Now, isn't it true that a Silk Road user would have communications -- withdrawn.

doing is looking at the movement of bitcoins back and forth, correct, from Silk Road servers, right?
A. Not back and forth. Just one direction from Silk Road to the Ross' laptop.
Q. And you mentioned --
THE COURT: I want to make sure that you don't speak over the witness.
MR. DRATEL: I'm sorry.
Q. But you mentioned that the amount that was in the FBI wallet was actually larger than the amount that was in -- that was transferred from the laptop, right?
A. Yes. So once the transaction -- once the seizure happened, FBI address made it onto the block chain and transaction of that size normally gets noticed by a lot of bitcoin users. So once that happened, the government seizure address was publicly known at that point. And just like -- just like an email, someone could send you an email and you send end up receiving it, whether it's spam or not. So we received a lot of small transactions that also came into the government wallet -- government address.
Q. Bitcoin?
A. Small -- fractions of bitcoins.
Q. But you don't know where they were from necessarily, right, you didn't track them all down?
A. I'm sorry. What was that?

voluminous," again can you split them between the two groups? Are these really for the expert or are they other? Are they for the seven?

MR. DRATEL: I don't think the character/fact witnesses have exhibits necessarily. Maybe one, maybe a couple of things -- it's possible one or two pieces.

THE COURT: In terms of the expert, I take it that you have to have given the proper disclosure in any event to the government and that's all done.

MR. DRATEL: Yes. We have one expert that we're going to disclose probably later tonight based on what happened today.

MR. TURNER: On the expert, we're actually going to move to preclude. We don't believe the notice is sufficient.

THE COURT: Preview for me, is it because you don't think the notice is sufficiently detailed or for some other reason?

MR. TURNER: Three reasons: We don't think that the subject matters of the testimony requires specialized knowledge, we don't think they're relevant to the case and in any event, the expert disclosure does not even provide the opinions that this expert is going to provide. It just lists subject matters, very general topics of discussion and there's very clear law it's not sufficient under Rule 16, so we prepared a submission. We were going to file it with the Court

shortly after we get back.

THE COURT: I'll wait to see it. And that will increase the workload of the defense in terms of needing to respond to it because I'll need to rule on that very quickly on Monday morning. It will be an initial order of business at 9:00 a.m. So let me see when yours comes in. And if you can confer with the defense as to timing on when they can respond and recite that, that would be helpful. If you can't, then Mr. Dratel, if you can let me, as soon as it's filed, have a sense Tuesday the soonest you can get it.

MR. DRATEL: Yes.

THE COURT: Because I don't want to give you a deadline --

MR. DRATEL: Understand. I understand.

THE COURT: But I'd like to be able to read both. What's the topic of the expert?

MR. DRATEL: Bitcoin.And the other expert is the Computers, these computer issues.

THE COURT: Let's deal with these as they come in. I take the heads-up Mr. Turner now. Now, in terms of numbers of -- in terms of exhibits, let's assume for the moment because I want to work on the logistics as well and I just don't know how any of this is going to come out: When is the time frame that you need the exhibits by?

MR. TURNER: I think any expert witness we would need

them sooner rather than later. The fact witnesses, the character witnesses are less of a concern.

I would add this is extremely late for disclosure of another expert witness so we would hope that that disclosure is made very promptly.

THE COURT: Well, if it's coming out of today with Mr. Yum in terms of his analysis, that's one thing and we'll deal with it when we see what the notice is; and you folks, if you've got an issue, you'll raise the issue and the defense will respond.

MR. TURNER: I was speaking of the second expert, the computer issues expert.

THE COURT: He said it was coming out of --

MR. DRATEL: I'm sorry. I may have misspoke. It is coming out of a series of witnesses, some of whom testified I think as late as yesterday, but it also has to do with some of the limitations on cross that have occurred in the last couple of days. So you say we have to call a witness, we'll call a witness.

THE COURT: Well, I said we would take up the application if you're going to call a witness. So if you need to call a witness and you're going to attempt it, it doesn't mean you get around the Rule 16 disclosure requirement. So you'll work with the government, make your disclosures. If the government has a problem with it, they'll raise it with me and

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA,

v. 14 Cr. 68 (KBF)

ROSS WILLIAM ULBRICHT,

Defendant.

----------x

New York, N.Y.
February 2, 2015
9:10 a.m.

Before:

HON. KATHERINE B. FORREST,

District Judge

APPEARANCES

PREET BHARARA,
United States Attorney for the
Southern District of New York
BY: SERRIN A. TURNER
TIMOTHY HOWARD
Assistant United States Attorneys

JOSHUA LEWIS DRATEL
LINDSAY LEWIS
JOSHUA HOROWITZ
Attorneys for Defendant

- also present -

Special Agent Vincent D'Agostino
Molly Rosen, Government Paralegal
Nicholas Evert, Government Paralegal

THE COURT: All right.

MR. DRATEL: As the Court is aware, the government's initial exhibit list and throughout the first half of the trial included Andrew Jones, who has pleaded guilty to his involvement in Silk Road as an administrator under the name of inigo. At some point midway through the trial, the government said they may not call him and then just last week conclusively told us that they would not call him.

When it initially became -- when I was initially informed that he would not be called by the government, I spoke with Mr. Turner about a specific piece of *Brady* material that the government provided. The government doesn't call it *Brady* because they don't call anything *Brady*.

Mr. Turner in a telephone conversation with me and Ms. Lewis said there is no *Brady* material in this case because he believes the defendant is guilty, so that's his view of *Brady*. So the notion that the government understands its *Brady* obligations is not reliable in this case.

So I asked him if he would stipulate to the piece that he knew we were interested in and he said yes, just a matter of language. Then I asked him again when he said that -- when they concluded they would not call Mr. Jones and he agreed again to stipulate. And then over the weekend yesterday I gave them the language of the stipulation which is only what is in their letter with the exception of one sentence which was

removed; it's only what's in their letter. And I got back -- and then I spoke to Mr. Turner at 7:00 last night and he at first resisted unless I met one of his conditions on something completely unrelated that he would not stipulate unless I made met a condition that was completely unrelated. I agreed because this stipulation is that important to his condition. And then at 11:00, he writes me an email saying they're not stipulating.

THE COURT: Why don't you describe to me what the substance of the issue is.

MR. DRATEL: Yes.

THE COURT: Because it sounds like the alternative would be to call Mr. --

MR. DRATEL: Can't call him. He's going to take the Fifth Amendment. I spoke to his lawyer. He's unavailable. So I would move it, by the way, either as a statement against penal interest, 807, defense witness immunity. I'd ask for all those things. This is a case where if ever there was an appropriate case for it, this is it.

So on December 29, 2014, we received a letter from the government and on the second page of the letter it says that in a recent witness interview, Andrew Jones a/k/a inigo said the following, and this is the quote. This is not necessarily a quote from Mr. Jones but this is the government's characterization of what he said.

THE COURT: It's a 302?

MR. DRATEL: No. It's not a 302, but this is a letter from Mr. Turner, signed by Mr. Turner:

At some point in or about August or September 2013, Jones tried to authenticate that the Silk Road user "Dread Pirate Roberts" whom he was talking to at the time (via Pidgin chat) was the same person with whom he had been communicating in the past with this username. Previously in or about October 2012, Jones and "Dread Pirate Roberts" had agreed upon a "handshake" to use for authentication in which Jones would provide a certain prompt and "Dread Pirate Roberts" would provide a certain response. When during the 2013 chat in question Jones provided what he believed to be the designated prompt, "Dread Pirate Roberts" was unable to provide the response Jones thought they had agreed on; however, later in the chat, Jones asked "Dread Pirate Roberts" to validate himself by specifying the first job that "Dread Pirate Roberts" assigned to him (running the 'DPR book club') which "Dread Pirate Roberts" was able to do.

And then that's the block quote, and then the last paragraph is: The government is unaware of any extant record of the 2013 chat described by Jones. There is a record of an October 2012 chat between the defendant and Jones discussing a "handshake" in the file labeled MBSOBZVKHWX4HMJT on the defendant's computer, which has already been provided to the

defense in discovery, and our stipulation would have included that specific chat, which is very short -- I think it's one page basically-- as part of the stipulation.

THE COURT: Mr. Turner, why has the government taken the position it has on the stipulation?

MR. TURNER: First of all, your Honor, I just want to be clear, I never said that we would stipulate. What I said is that we would consider stipulating. And what happened was this disclosure was made over a week and-a-half ago and the defendant did not get proposed language to the government until last night when the government was very, very busy with other things. The language that the defendant proposed for one thing omitted the very last sentence the defense counsel just read, which is, in the government's view, clearly important because the point is that inigo, Mr. Jones, tried a prompt that didn't work but then he tried another prompt that did.

THE COURT: Then you could add that in. That would be the product of a negotiation over the language of the stipulation.

MR. TURNER: The problem that I had is that, like I said, this came at the 11th hour.

THE COURT: Can you look at it this morning as we're proceeding?

MR. TURNER: I can, although it's not my job to draft appropriate language.

THE COURT: No. Mr. Dratel, it sounds like, has done that job. He's drafted language. Why don't you take a look at it and see whether or not there are additions that you could make to it or changes you could suggest that would then make it acceptable to the government.

Only at that point when I've got the two of you having truly joined issue do I want to have to then make a ruling. If you folks are able to agree, then that's obviously the best course.

Will you do that?

MR. TURNER: We will. To make it clear --

THE COURT: I understand you don't want to.

MR. TURNER: No, I just think just quoting what we put in a letter does not provide necessarily sufficient context by itself.

THE COURT: Go back and figure out what the context is that's fair. You folks then negotiate over this. We still have the government's witness on direct and I think Mr. Howard said he's got an hour or two left with that. Then there's cross. So you have some time while you're sitting there maybe to take a look at this.

Mr. Dratel, do you have it in a form written or otherwise that he could look at and fiddle with?

MR. DRATEL: I sent him the stip. I have it here.

THE COURT: In paper copy.

MR. DRATEL: I can give it to him. I can give him my copy. I know what it says. And so we're clear, Mr. Turner's response to me last night was he couldn't consider alternative language and it was too late to do so and he never made a plan or proposal. The reason I took that sentence out -- so we know where we're going, the reason I took that sentence out is because they could have called him to get that. It's a confrontation issue with respect to that. There is a confrontation issue. If there's a completeness issue, that's a different issue, but they never came back with a single sentence that's not in there. Everything else is from the government's letter. This has never been a mystery. We're talking about preparation time. This has never been a mystery as to what we want to do.

THE COURT: I hear your position. So I'm going to ask the government to look at that and see if there are additions or changes which would make it acceptable.

If the answer is after further considering the matter there are not, then we will deal with it in that posture. But if there are further changes or modifications that would make it acceptable, I'd like to know that.

Are there any other matters, Mr. Dratel?

MR. DRATEL: I prepared some supplemental requests to charge, they're very short, based on evidentiary issues. If I have a representation from the government that this is the

THE COURT: Mr. Dratel, do you want to respond to the government's letter on Defense Exhibit E?

MR. DRATEL: The letter is filed under seal, your Honor.

THE COURT: The issue I think can be described as follows. It's I think number one, whether or not the purpose of the document is for the truth and if it's not for the truth, then what other purpose does it serve?

And then there's certainly an issue which we can talk about in open court, in fact, I think we can talk about all of it in open court, except for the one issue that has been under seal throughout the entire case, but everything I think can be referred to other than that. The second point, if it's not offered for the truth, goes to the issue of the *Wade*, what I'll call the *Wade* issue about other perpetrator evidence.

MR. DRATEL: It doesn't go for the truth in the sense of the information in it; it goes for the truth the fact that it was communicated to DPR, which is indisputable in that this particular piece of evidence communicates to DPR the name and profile of the person deathfromabove believes is DPR, and that's what he says the information is.

Now, I don't know if I can go further or not go further in open court, but the fact is, the government has created a situation and now they want to profit from it by precluding evidence and also saying that the other parts we

redacted, we redacted because they won't let us use it. They redacted. They took that part out of the case, so I don't understand how they can possibly have it both ways.

THE COURT: Let's forget about the redactions for a moment. Let's just focus on if the information between these two declarants is offered for the truth, in other words, if you want to offer it for the truth that Anand is the perpetrator --

MR. DRATEL: It's not offered for the truth. It's offered for the fact that DPR was getting information about people who were supposed to be DPR and that these things were coming in. There's a whole law enforcement file that's part and parcel of the whole thing. And one of these people is one of the people who the agent was investigating.

I think it's a fair inference. I think it's a completely fair inference for anyone to draw.

THE COURT: The first part that I want to take is just sort of the hearsay part whether it's for the truth or not for the truth. So if it's not for the truth, in other words, if the defense doesn't intend to say Anand did it, the real DPR was Anand -- if the defense is intending to say the real DPR was Anand, then this is obviously for the truth.

MR. DRATEL: No.

THE COURT: Tell me whether or not you're planning on making --

MR. DRATEL: It's not that; it's that if you're DPR

and you get a name, a specific name, this Anand Athavale and a profile and details, if it's Anand Athavale, if it is, and you're put on notice that it's you, you're going to take steps, so that's not saying that it's him.

THE COURT: That's used for the truth.

MR. DRATEL: No, it's not for the truth; it's the fact that he was informed, it's the fact that DPR was informed. That's indisputable. It's not for the truth of whether it is or not. It's for an inference for the point is that if DPR is informed that it's him, then he's going to take action. And that's not for the truth of the matter of whether it is or not; it's for the purpose of drawing an inference that anyone who -- and also the fact that if DPR is getting information from law enforcement about specific people, he knows the walls are closing in, he's going to take action to implement an escape plan. That is just a fair inference from all of that.

THE COURT: So the theory would be that Anand Athavale understands by virtue of his exchange that investigative sites are trained on him and he takes evasive actions in response thereto.

MR. DRATEL: If it's him. And I'm not going to say it's him. I'm going to say anyone in that situation and even DPR even, if it's not Anand Athavale, DPR is very interested and clued in as to what is going on in the law enforcement community and he is actively security-conscious in a very

substantial way and that's an inference that we're -- it's not even an inference. It's a fact from this.

THE COURT: So what evidentiary basis is there that there was another DPR? And what evidentiary basis is there that the defendant ever handed off Silk Road and then took back Silk Road as a setup that would then demonstrate the existence, by inference at least, of an additional perpetrator?

MR. DRATEL: Well, the evidence that he gave it up is that Richard Bates testified to that. The government's own witness testified to that.

THE COURT: That he told that he had given it up?

MR. DRATEL: Yeah.

THE COURT: What is the evidentiary basis that there was a handoff to anyone else?

MR. DRATEL: Well, that's a series of pieces of evidence.

THE COURT: Such as?

MR. DRATEL: I don't want to sum up before they sum up.

THE COURT: Under the *Wade* case and other case law for the Court, as you know, the Court must undertake an analysis as to whether or not other perpetrator evidence is going to result in inviting jury speculation and there must be a substantial connection between some other potential perpetrator and the facts before the Court. You can't just throw up names and

other possibilities. The courts have long said that that's an inappropriate way to proceed. There's just lots of case law on this point.

We're waiting for two more jurors.

MR. DRATEL: The government -- on Thursday, Agent Shaw showed that there is a second administrative key, the SSH key, that gives someone completely separate from even frosty, assuming that that's Mr. Ulbricht, access to the server. I believe that the Government Exhibit 130 and the thumb drive also are --

THE COURT: The thumb drive found on his night table?

MR. DRATEL: Right.

THE COURT: Why would that possibly result in anything other than incriminating him?

MR. DRATEL: Because why would it be on the thumb drive if it's on a laptop? It's on a thumb drive because that's what was given to him, and that's an inference that the jury is entitled to draw.

THE COURT: That sounds like the difference between an inference and speculation. Let me gather what you believe the evidentiary basis is for another perpetrator. It's Bates that he was told that Ulbricht had given up Silk Road, and it was the second administration key, which is not tied to somebody who was calling themselves -- well --

MR. DRATEL: There were changes in the site throughout

that would indicate that there was a change. You have the origin of DPR in general, the changes in October of 2011, the changes in June of 2011, the changes in January 2012.

THE COURT: You need to come up with something that is a handoff to another person by inference; otherwise --

MR. DRATEL: But Bates said he sold the site and that it was no longer his problem as of 2013. The standard is not that I have to prove it's someone else. The standard --

THE COURT: The standard is you have to show a substantial connection that there is another perpetrator.

MR. DRATEL: No. I think I have to show a substantial connection to this case, not to another perpetrator specifically. That's a burden on the defense that doesn't exist.

THE COURT: It's a substantial connection that that other person is, in fact, the true perpetrator of the crimes charged here.

MR. DRATEL: Well, that's what I was trying to get to in my cross-examination of Agent Der-Yeghiayan. I would have gotten to it also with other witnesses, but I was precluded from cross-examining them on this.

THE COURT: For instance, is there evidence --

MR. DRATEL: The Jones handshake in September 2013, August or September of 2013, the handshake evidence is critical in this. It's not in yet, but it's critical. You talk about

handoff at the end, that's an inference that we're entitled to have.

THE COURT: Let me hear from the government.

MR. HOWARD: I believe the *Wade* case requires more of a substantial connection between the actual alternative perpetrator that they're trying to depict, not just someone else generally. Here the issue is that to the limited extent -- to the extent this has any probative value, it is if exactly as if Mr. Athavale is the alternative perpetrator. There is no evidence which substantially connects him to a theory that he's an alternative perpetrator in this case for the reason we set forth in the letter.

THE COURT: Defense Exhibit E is precluded on the basis that it's hearsay. It is offered for the truth that Anand is the DPR or that Anand is one of potential other DPRs, which makes it for the truth, and I can't find any reason that it would be offered other than for the truth.

The *Harwood* case, 998 F.2d 91 deals with a situation where information which comes in that's irrelevant, unless it's for the truth, is applicable as well as other cases. Let me give you another one. There are legions of cases that are supportive of keeping things out which are coming in for the truth. And based upon everything I have heard, the use of this would be for the truth. Therefore, it makes the statements as between two out-of-court declarants, and you can't just have

two out-of-court declarants, offered for the truth.

Also even if it wasn't offered for truth, you then get into the secondary analysis of the *Wade* standard. The *Wade* standard relies upon the *McVeigh* standard, and it says "In the course of weighing probative value and adverse dangers, courts must be sensitive to the special problems presented by alternative perpetrator evidence. Although there is no doubt that the defendant has a right to attempt to establish his innocence by showing that someone else did the crime, a defendant still must show that his proffer evidence on the alleged alternative perpetrator is sufficient on its own or in combination with other evidence in the record to show a nexus between the crime charged and the asserted alternative perpetrator. It is not sufficient for a defendant merely to offer up unsupported speculation that another person may have done the crime. Such speculative blaming intensifies the grave risk of jury confusion and invites the jury to render its findings based on emotion or prejudice." That's cited in the *Wade* case, Second Circuit, binding on this Court, 333 F.3d 51, pin cite at 61. So that issue is resolved.

How are we doing with the jurors? Still waiting on two.

(Continued on next page)

BY MR. DRATEL:

Q. That is talking about security, correct?

MR. HOWARD: Objection.

THE COURT: Sustained.

He can't talk about what the content means. He can talk about what the content is on the page but he can't interpret the content. So, move on.

MR. DRATEL: Your Honor, this is a witness who put the document in evidence.

THE COURT: He did. He did put it in evidence. He can't interpret what the people meant.

BY MR. DRATEL:

Q. Let's go to April 2nd, 2013 at 20:55, page 24.

A. Okay.

Q. And that entry which is in the middle of the page, if we can blow that up a little bit it says:

"Regarding image metadata, you can strip all of that out and it is a good practice. The upload page is secure, but I would still have access to that metadata."

By the way, this is from Dread Pirate Roberts to redandwhite?

A. Correct.

Q. So:

"Regarding image metadata, you can strip all of that out and it is a good practice. The upload page is secure, but

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

UNITED STATES OF AMERICA,

v. 14 Cr. 68 (KBF)

ROSS WILLIAM ULBRICHT,

Defendant.

----------x

New York, N.Y.
February 3, 2015
9:10 a.m.

Before:

HON. KATHERINE B. FORREST,

District Judge

APPEARANCES

PREET BHARARA,
United States Attorney for the
Southern District of New York
BY: SERRIN A. TURNER
TIMOTHY HOWARD
Assistant United States Attorneys

JOSHUA LEWIS DRATEL
LINDSAY LEWIS
JOSHUA HOROWITZ
Attorneys for Defendant

- also present -

Special Agent Vincent D'Agostino
Molly Rosen, Government Paralegal
Nicholas Evert, Government Paralegal

have then taken care of the one, are where we are.

Are there things which you folks would like to raise?

MR. TURNER: No, your Honor. I responded to the inigo issue.

THE COURT: Mr. Dratel, anything from your perspective you would like to raise in addition to those items?

MR. DRATEL: No.

THE COURT: In terms of inigo, I have received the letter from defense counsel. Let me just preview that I think it breaks into analytically into two very separate inquiries though they're related: One is the hearsay issue relating to reading into the record the statement that inigo, a cooperating witness, gave to the government and as recounted in the letter of December 29. So there's the hearsay issue and then there's a separate request for a missing witness charge in the event that the statement is otherwise disallowed. So I think analytically those are related but stand separately.

Mr. Turner, I didn't receive a written response from the government. I knows you folks are busy, but why don't you tell me your views.

MR. TURNER: Sure. As the government sees it, this is sort of another example of the defense assuming they can get in their case through our witnesses. So the defense has known for approximately two weeks that we were not going to call Mr. Jones. They made no effort to contact or subpoena

Mr. Jones until the eve of the defense case. They didn't ask us to immunize him. They made no effort to draft any stipulation even though we told them that we were open to a stipulation until the eve of their case. And now the defense is trying to use the lack of time, which is an issue of their own making, to try to force the government to agree to whatever stipulation language the defense wants, even though it does not include language that is favorable to the government.

Defense counsel had no right to assume that he'd be able to rely on a stipulation to get in facts they want from Mr. Jones. You have to have a witness lined up in case a stipulation falls through. That's why for Alex miller with Stack Overflow, we wanted to get that in through stipulation. We weren't able to work that out. We had Alex Miller ready to testify. They were obliged to do the same thing with Mr. Jones.

Defense counsel is trying to make it out as we engaged in some sort of tactical maneuver by not calling Mr. Jones. We didn't call Mr. Jones because we felt like we no longer needed it for the case. That was our right. That was our call. And the defense was not entitled to rely on our calling a witness during our case and them getting in some fact from Mr. Jones through his testimony on our case.

The confrontation issue that they have tried to raise is ludicrous. This is a stipulation we're talking about. So a

stipulation can present any statements that the witness would be able to testify to. And it would be perfectly appropriate if he were to testify about this conversation he had to explain his understanding of the conversation, to explain his state of mind during the conversation. It happens all the time when you have witnesses testifying about conversations they're having with other people and what's going on, the context of those conversations. That's all we were trying to put in this stipulation and the defense didn't want that in. We think it's necessary to be balanced.

So if they're not amenable to a stipulation, then it's up to them to call the witness. You can't just get in core hearsay because the government won't stipulate to putting information in a stipulation. You can't just take a letter that the government sends, which is not the declarant's statement, that is the government's disclosure, that is the government's characterization, that's not been adopted by the declarant, so you can't just ignore the hearsay rules and just submit a letter.

THE COURT: Let's go to the hearsay rules. As I said, I think this breaks analytically into two pieces, each of which have their own independent evidentiary standards. One is 8043, there's a typo in defense letter but we understood from yesterday what he was referring to, so it's not 803. It's 8043 which is a statement against penal interest, which is an easy

juxtaposition to make, that statement against penal interest, as the Court understands it, requires two parts: It requires subpart A and subpart B. Subpart A requires a statement against penal interest, which typically is a statement made under circumstances which indicate that no person would have made it unless they were telling the truth because it was so contrary to their interest under those circumstances to do so. And it also requires B, which is big letter B, B also requires some independent corroborating evidence as to the trustworthiness and/or reliability.

Why don't you address whether or not, putting aside the circumstances over not reaching the stipulation, whether or not the hearsay statement otherwise meets the standard under 8043.

MR. TURNER: First of all, it's not his statement. It's not like an email that he sent. It's not an affidavit he signed.

THE COURT: No. It's your recitation of his statement.

MR. TURNER: That is hearsay.

THE COURT: I understand we're dealing with hearsay. I'm saying tell me why it doesn't fit within the hearsay exception.

MR. TURNER: The point is, it's not just the declarant's statement; it's somebody else's statement about

what the declarant said, so it's double hearsay.

THE COURT: Lovely.

MR. TURNER: And that's part of the problem. That's a characterization of what this declarant said. It's not the statement itself.

THE COURT: So we go to both pieces of it, okay.

MR. TURNER: Right.

THE COURT: Mr. Turner, I'm trying to cut through because let me be perfectly blunt: I don't think this meets the hearsay standard. I don't think under 8043 this is a statement against penal interest. The reason for that is because the witness at the time was already under a cooperation agreement.

Under a cooperation agreement, under Second Circuit law, there is clear law that says that you're no longer under criminal penalty for making a particular statement; (B), based upon the representations of the government, there's no corroborating evidence for reliability because there's no chat that ever indicates apparently that this ever happened. There's no indication in the record so far that there is an absence of chats and, therefore, the absence here, there's just nothing to corroborate this as a reliable statement. So I don't think it meets 8043.

Do you disagree with my analysis?

MR. TURNER: We absolutely disagree, and we just also

believe there are further reasons that it doesn't even come under 8043 to start with because it's not this witness' statement. It's the government's statement about what he said.

THE COURT: Why don't you go to the missing witness charge, which I think is analytically separate.

MR. TURNER: Again, this is an issue of the defendant's own making. If they wanted to call this witness, that's something they should have realized right after they learned we weren't going to call him. If they thought he was that important to their case, they should have asked can we immunize him, can we call him. That could have been worked out two weeks ago.

THE COURT: Would you have immunized him or is this sort of an argument that you can make because they didn't ask but you would not in fact have immunized him?

MR. TURNER: No. I'm not representing that at all. I think we would have immunized him. He's under our control and we would not have resisted allowing him to testify. The point is, even a stipulation was not proposed until the eve of the defense case when government counsel was busy preparing for closing, preparing for possible cross of the defendant, preparing for the witnesses that were going to be part of the defense case.

This was sprung on the government on the last minute. It's an issue of the defense's own making and to say that, oh,

now there's an unavailable witness because they don't have time now to scramble and subpoena this witness and work out the immunity issues, it's their fault.

THE COURT: Let me ask you, I thought that Mr. Dratel had information that indicated this witness would take the Fifth if called.

MR. TURNER: Apparently he called his counsel, he didn't call me, he called -- this is just based on what Mr. Dratel said in court, I didn't even talk to counsel for Mr. Jones since then. But I understand that he called counsel for Mr. Jones and counsel said, well, he'd take the Fifth. But defense counsel can still contact the government and see if we would immunize the witness so that he couldn't claim the Fifth Amendment. We never had that discussion. We were never consulted about that.

MR. DRATEL: It's not the government's position to immunize a witness. It's the Court's authority under the statute. The government has never immunized a defense witness, never.

THE COURT: They make an application, which is then so ordered by the Court but typically it's within the prosecutorial discretion as to whether to suggest immunization, so they are related.

MR. DRATEL: That's the most specious argument, the most disingenuous argument I have heard. This is completely

outrageous. By the way, last weekend we were told that Mr. Turner would not agree to anything and would not discuss anything with us, and that's what we were told last week. I'm just -- I want to call Mr. Turner as a witness. We'll eliminate the double hearsay problem. He wrote the letter and signed it. He's disavowing it. This is so disingenuous, so outrageous. A prosecutor has obligations that transcend wanting to win the case at all costs, and this is what we have here.

THE COURT: Let's take these two issues analytically separately; one is the hearsay issue whether we think of it as single hearsay or double hearsay, 8043, whether or not those standards are met.

MR. DRATEL: Yes.

THE COURT: If they're not met, then we are into the world of the missing witness charge. If they are met, then there is some other issues as to whether we can read it in.

MR. DRATEL: Two things: One is, it is a statement against penal interest. He is not sentenced. All of these things can be raised at sentencing. That's why he has a Fifth Amendment privilege is because the statement against penal -- even if he's cooperating, and the truthfulness and the trustworthiness aspect of it, there's a chat that substantiates the first part of it, so that indicates the trustworthiness. They went and found the chat. They didn't have the chat

beforehand. They went and found the chat which substantiated the first part, and he is under an obligation to tell the truth or else he loses his cooperation agreement. Every jury is told that and argued by the government why would -- they're going to argue it here with respect to Mr. Duch. They're going to argue it here with respect to Mr. Bates. They're going to say this guy has an agreement. He would never lie to you. What more trust -- they can't have it both ways.

They continually want it both ways. This is a preposterous argument. I want a page and-a-half stipulation that they don't have time to read. They knew exactly what was in the -- my stipulation is completely what's in the letter. And what I objected to in their stipulation is what they're not entitled to. They could have called the witness if they wanted balance.

THE COURT: Hold on. I want us to pull back and take a deep breath and focus on --

MR. DRATEL: It's just an outrage. That's all. It's an outrage.

THE COURT: I hear what you're saying. I do want us to focus on the evidentiary rules because --

MR. DRATEL: Part of it is fairness. Part of it is *Chambers v. Mississippi*. Part of it is due process. Part of it is they can't do a bait and switch. I called the lawyer. He's on trial, by the way. I called him on the weekend and he

told me he's taking the Fifth.

They never offered -- this immunity is preposterous. You should ask them right now. He's said no, we're not saying we're going to immunize him. Of course not, because they're not going to. This is a bogus argument, bogus, bogus, bogus, and it's coming in a way that is completely disingenuous.

He should be a witness, and it's a problem 100 percent of his making because they had him on the witness list. In the middle of trial, they say he's not testifying. He's the best witness; Mr. Turner wrote the letter. He heard the statement. He was there.

THE COURT: You folks are sufficiently emotional about it. I have the government's statement. I have your letter. I have read your letter. I have also looked at case law. Let me be sure that I understand the chats which do exist versus the chats which don't exist.

As I understand it, the chat which does exist is the October 16, 2012 chat which indicates the "recommend a good book Rothbard" answer, that that chat has been found.

MR. DRATEL: Correct.

THE COURT: I understand that paragraph C, which is really the heart of what we're discussing here, the chat as to whether the key identifying question was asked, that chat has not been found.

MR. DRATEL: Because it was a Pidgin chat, which are

not saved. It's different. It's a different type of chat.

THE COURT: There are some.

MR. DRATEL: Well, not the Pidgin chats, no.

THE COURT: Here, let me just tell you my ruling on the 804(3) issue. On the 804(3) issue, putting aside the double level of hearsay, just assuming that this is a faithful representation of what the witness said, it's an out-of-court statement; without a doubt it's being offered for the truth. It has to meet both provisions of 804(3).

I do not believe that it was against the declarant's penal interest as the case law interprets it because he was under a cooperation agreement at the time. Moreover, the chat itself independently and in itself doesn't carry any particular penal impact; in other words, it's not the equivalent of a statement saying I sold the drugs or the equivalent of saying I did X, Y or Z. It's simply whether or not a particular communication occurred. So it does not meet some of the circumstances that are anticipated under (A).

Under subpart (B), it also needs to be -- and there's an "and" between those subparts -- corroborated by circumstantial evidence clearly indicating its trustworthiness. Its trustworthiness is not whether or not it was said to Mr. Turner. Its trustworthiness is whether or not it ever occurred. There's nothing that I'm aware of that indicates the trustworthiness as to whether or not it ever occurred.

Therefore, it is not a hearsay statement which can come in under 8043.

Under a missing witness charge, I've received the government's now oral response and I've also looked at the defendant's papers. Important in this regard are several Second Circuit cases, which the Court pulled this morning. One is the *Myerson* case, 18 F.3d 153 at pin cite 159; the other is the *Burgess v. U.S.* case, which is a DC circuit case -- the *Myerson* case is a Second Circuit case -- the *Burgess* case is a DC circuit case which is quoted at length in the *Myerson* case favorably. That's at 440 F.2d 226. And then there are a series of other cases. There's the *U.S. v. Torres* case, Second Circuit, 845 F.2d 1165, pin cite 1169 to 70.

In the *Myerson* case where there's a question about a missing witness, the Court is to look at a series of things: One the relation of the parties, not only physical availability, and I think that there are some questions as to whether or not there was in fact true physical availability which would include the immunity issues and everything else, but the Court does note the special relationship between the parties by virtue of the cooperation agreement and that, therefore, there is some further ability by the government to control this witness.

Whether or not that the defense did all that it could have I think is open to question but, frankly, I'm more

persuaded that the government does have control over this witness. That does not end the analysis. That just clears us to the point where we're able to ask the substantive question. The substantive question is whether or not -- and by the way, immunity is only given under extraordinary circumstances and I don't think that immunity here would be extraordinary circumstances.

But putting that aside, the question really is, and I'm quoting from the Second Circuit, "When the court is asked to give the instruction, then a judgment is to be reached as to whether, from all the circumstances, an inference of unfavorable testimony from an absent witness is a natural and reasonable one."

From the *Burgess* case, I'm going to recite a longer paragraph because it gives really the basis for what all of the circuit courts do in this regard and it's the *Burgess* case is widely cited for setting this standard.

"When the court is asked to give the instruction, then a judgment is to be reached as to whether, from all the circumstances, an inference of unfavorable testimony from an absent witness is a natural and reasonable one. In reaching a decision, the court will have in mind that it is not ruling upon an offer of evidence. The missing witness instruction is not evidence, but is concerned with the absence of evidence. While the context in which the question arises may clothe the

missing witness with significance, there is the danger that the instruction permitting an adverse inference may add a fictitious weight to one side or another of the case. When thus an instruction is sought, which, in a sense, creates evidence from the absence of evidence, the court is entitled to reserve to itself the right to reach a judgment as wisely as can be done in all the circumstances."

It is the Court's view having looked at the proffered language, and assuming that the witness, if called, would testify to that language, is that this is not reasonably exculpatory when all things are considered. This witness says he asked a first question. There's no indication that it was not answered -- I guess the only implication is it was not answered. There's no implication that it was answered wrongly. There's no implication as to whether or not multiple things were going on at the same time. Eleven months had passed. A second question was then asked to reveal identity, just as Google does to reveal identity of people all the time where you get three or four different questions to figure out what your first dog's name was, that second question was answered correctly; and therefore, the only reasonable inference to be drawn from this is that the DPR identification was completed. Any other inference would be, in this Court's view, an unreasonable inference, so the inigo issue is resolved. There will be no missing witness instruction on that issue.

MR. DRATEL: Then I'm signing the stipulation that the government proposed.

THE COURT: Go ahead. Do you want to agree to the stipulation?

MR. DRATEL: He already did. He proposed it to me.

MR. TURNER: Let me just consult, your Honor, over the break.

THE COURT: That's fine with me. If you stipulate to facts, that takes it out of the Court's hands, then I have no reason to make an independent evidentiary ruling.

Now, on the jury instructions, we will accept the defense jury instruction on the character evidence with the addition of two sentences from the Sands instruction. Sands for character evidence also includes -- I don't have the exact language right here, but it's essentially, here it is, the testimony is not to be taken by you as the witness' opinion as to whether the defendant is guilty or not guilty, that question is for you alone to determine.

So it will say an independent -- there will be an independent instruction on character: You have reputation evidence about the defendant's character trait for peacefulness and nonviolence. This testimony is not to be taken by you as the witness' opinion as to whether the defendant is guilty or not guilty. That question is for you alone to determine. You should consider character evidence together with and in the

(In the robing room)

THE COURT: All right. So we've got Mr. Turner, Mr. Howard, Mr. D'Agostino, Mr. Dratel, and we are on the record in the robing room.

Mr. Dratel, has your client waived his appearance?

MR. DRATEL: Yes, he has, your Honor.

THE COURT: Thank you.

I have before me Defense Exhibit C and N. As I understand it, as to C, and C only, there is a particular issue which the government wanted to raise in camera. So that is the purpose for having this session.

I have now reviewed this document, but it is a lengthy document with single-spaced text. So let me just say that I get the gist of the document, that somebody is providing or appears to be providing DPR with inside information on to -- with regard to the investigation.

MR. TURNER: Yes, your Honor, the investigation -- I want to state, to be clear for the record, the Baltimore investigation, not New York's investigation.

This is yet another effort to try to inject Carl Force into the case. This Al Pacino or Albert Pacino that has already been disclosed. He is under investigation as being Carl Force. This is utter, rank hearsay. It is hugely prejudicial, because it says all sorts of things about government investigators. It says things about the Mt. Gox

issue that I'm sure the defense will want to highlight and present for the truth, or insinuate for the truth in some manner. That we have no idea whether it is reliable or not. You get into the issue of the alternative perpetrator issue again, that you cannot rely on certainly not inadmissible evidence and certainly not evidence that continues to lack any specific, create reflection of a true alternative perpetrator.

Instead, this is just some guy leaking information that he's getting from God knows where to DPR in order to get into his good graces so he could get money. And it prejudicial. It could be interpreted by the jury in so many prejudicial ways. It could be interpreted to mean that possibly Agent Der-Yeghiayan was the one who leaked this information. There is stuff in here about how federal agents are sloppy, they're greedy, etc., etc., etc., all sorts of prejudicial statements about government investigators.

There are statements about like the sort of person DPR is expected to be, what his profile is. It says in here at one point you are suspected to be 30 to 35 years old, living on the East Coast. I'm sure they are going to try to point to that as now Mr. Ulbricht doesn't fit the profile.

It is ridiculous. It is not competent evidence about anything. This is again trial by ambush. This has only been disclosed to us this morning. And enough is enough. They had time to come up with competent, real evidence of a defense

theory. This is just something to embarrass the government and confuse the jury and it should be denied.

THE COURT: All right. Why do you say -- let's explore the hearsay issue for a moment. Before I get to you, I just want to find out more about your view as to why it is hearsay, Mr. Turner.

MR. TURNER: Why is it hearsay, your Honor?

THE COURT: Yes. I just want you to state for the record. Rather than having me recite the reasons why you might be thinking it is hearsay, why don't you just make a record on the hearsay.

MR. TURNER: Sure. It is a document obtained on his computer that is called "LE Counter Intel," so it appears to be statements by someone providing counterintelligence on law enforcement. And it says things like "From East India Trader on forum." So that is from East India Trader. Then later it indicates that it's from Albert Pacino. So who knows what these statements are, but they are clearly not in-court statements of a testifying witness.

THE COURT: All right. Mr. Dratel.

MR. DRATEL: First, it didn't bother the government at all about what was in there when they designated it as an exhibit. So I don't understand their question about embarrassment and all of these other things. It is a government in the form that I am trying to put it in. So all

of that part is just really not an issue. That is a red herring and a distraction. I'm not --

THE COURT: Let me just understand it. Are you arguing that the government waived any hearsay objection by proffering it?

MR. DRATEL: No. But this question of prejudicial, 403, or all of that stuff is nonsense because it was their exhibit. This is their exhibit after they notified us about Carl Mark Force. This is after that. This is December 5th they gave us -- December 1st they gave us these exhibits. They wrote the Court and us on November 21st about that. So this is after. It nothing to do with Carl Force. Nothing.

It is about -- you know, this is all an attempt by the government to use that whole issue as a shield to keep out defense evidence. The rules I thought were that they could not sanitize what was already in the case. They just couldn't use the stuff that they gave us in that November 21st letter. But this is already in the case. This is on the laptop. They didn't redact it. It is nothing like that. They redacted the other one that they put in, 241. That they did redact, and we object to that, obviously, but we are bound by the rules that the Court stated with respect to the Carl Force issue. So that's a complete red herring.

The second is we are not putting it in for the truth.

We are putting it in because this is what was given to DPR. I opened on this on the basis of the fact that we were going to be able to use what was in the record before November 21, that we would be able to use this material. It goes to two things. It goes to DPR's knowledge about the law enforcement activity that causes him to be careful and cautious and also to be -- to implement an escape plan.

The second part, even separate from that, is the independent value it has to show the security consciousness of DPR about all of these things, and I'm going to contrast that with Mr. Ulbricht's conduct over the entire course of this case -- not the case in terms of the trial but in terms of the evidentiary portion of the case.

And so I believe I have a right to put that in to support that theory.

THE COURT: Let me understand. So you would not use this document in closing in any way to say, you see, here, highlighting, and then state it as fact?

MR. DRATEL: No, I would say this is what DPR was buying. This is what he was learning. This is why he did what he did --

THE COURT: Well, what was he learning suggests that he was learning a fact.

MR. DRATEL: No, but he was learning it -- we don't know -- you know, in other words, he could have thought of it

as a fact. I am not saying this independently, but it goes to the state of mind of the person who is receiving it. I mean, someone who is paying for all of this information and is getting all of this information is -- you know, it's having an impact.

So, I mean, the jury can infer that. I think that is a completely fair inference. And, you know, this is a problem of the government's own making.

THE COURT: Let me just ask you, Mr. Turner, whether there are particular things about the sloppiness of the government investigation or something like that which you think should, and on an isolated basis, be struck?

MR. TURNER: I think it goes a lot farther than that, your Honor.

THE COURT: I know you do.

MR. TURNER: For example, the timeline that was produced yesterday, that appears to be based extensively on this document, you know what's going on with Mr. Wonderful, what's going on with the Mt. Gox account. This is not an issue where an instruction can be relied upon to keep the jurors clear. The defense opened not on the idea that, oh, DPR was security conscious, that there was an alternative perpetrator.

MR. DRATEL: That's not true. I did both.

MR. TURNER: And that there was an alternative perpetrator and they tried to get to Agent Der-Yeghiayan and

Mt. Gox and Mark Karpeles. That I saw on the timeline. They are trying to take the references to Mt. Gox in here and make that suggestion to the jury.

If they want to -- if they are going to try to say, well, it is not for the true, it is just that Dread Pirate Roberts was aware that the government was looking at Mt. Gox, the jury is not going to make that distinction. The defense is going to continue to argue that there was an alternative perpetrator in the form of Mr. Karpeles; that's what this is come in for.

Again, it is rife with stuff that is objectionable.

And, you know, in terms of including it in the Government's Exhibit list, we discovered this long ago. We were gathering exhibits quickly. The fact that it was originally included means knowledge.

Certainly in the context of what we know about the defense case now and the alternative perpetrator theory they plan to present, this is the kind of garbage that they're trying to use to support it, and it's improper and it's extremely prejudicial to the government in the potential that the document has to confuse the jury. An instruction to the jury here is not going to be sufficient given the way they've opened and framed their case throughout. This is the one document that they're going to rely upon. It is the same agent belief issue, by the way. This is agents passing on secondhand

what other agents believed.

MR. DRATEL: It's not going in for the truth.

MR. TURNER: The defense says that, but, your Honor, that is the only -- that is the inevitable way that this document is going to be used.

MR. DRATEL: No,s it's not, number one. And I could make the same argument about all the documents that the government put in that were in for the truth. And we're bound by the rules. It is not coming in for the truth.

The fact is, you know, the government's arguments about the time line on their exhibits, I mean really.

The other thing is with respect to the alternative perpetrator issue, I do intend to argue that in summation based on the inferences in the record. There are inferences in the record. I'm not going to go beyond that. This should be in the record because this is a -- talk about ambush? I mean, they did not redact this document. They didn't start to make an issue of it with respect to Carl Force until today.

And, in fact, deathfromabove -- just so we're clear, on deathfromabove, the government never identified deathfromabove as being Carl Force. They never identified Carl Force as having the deathfromabove account. They only did that when we tried to put in Defense Exhibit E. That is the first time that came up. And in their footnote in their letter of the other day they basically seem to acknowledge that

deathfromabove is another one of Force's aliases, which is more Brady material that we haven't gotten and this investigation continues of him. So they're gathering Brady material as we try the case.

And, you know, I have to move for a mistrial based on that. It is just unconscionable at this point that we have a separate investigation going on where they are gathering Brady material for the defendant and we don't get to see it. It is directly relevant, and we don't get to see it, we don't get to use it. It is directly relevant to the issues in this case. These are documents that DPR has that he is given. So I am going to -- you hear my arguments, your Honor.

THE COURT: I hear your arguments. If that was a new application for a mistrial, then the application is denied. If it was just the old one --

MR. DRATEL: It was a new one.

THE COURT: Then I deny it. There are fewer in this trial applications for a mistrial than in our last trial. I think you were up to five there. You are only up to four now.

MR. TURNER: Your Honor, I would object additionally on the ground that we are hours away from closing. Your Honor set a firm deadline for the production of exhibits. This was not included. This is like 15 pages or so, single-spaced with stuff that is core, core hearsay, rife with accusations about all sorts of things that you would want to cross-examine the

person on. Huge reliability issues.

And the law is not -- the law is clear that there are situations where a jury instruction cannot be counted on to prevent the prejudice that could result from admission of an exhibit or testimony. And this is one of them. This is 15 pages of all sorts of hearsay, all sorts of wild accusations stuff that's being given for profit motive to DPR. No indicia of reliability. And, you know, this is just sort of reading material that, hmmm, this is interesting. Oh, look at this. They were looking into it there is corrupt Postal Service people. Look at this. There's -- I mean, this is so improper and so late --

MR. DRATEL: This is precisely the material that DPR was paying for. That is why it is relevant.

THE COURT: Let me ask whether or not you folks would be able to come to a stipulation right here, right now, to the effect that at X point in time DPR learned that the government was investigating Silk Road and the individuals behind Silk Road?

MR. TURNER: And you could even have a stipulation that there was law enforcement counterintel document on his computer. We would have no objection to that. But reading in all this --

MR. DRATEL: I will have to go through the document and see what is essential here.

THE COURT: But I would suggest that -- I think it's important that the defense be able to present something which indicates one of the legs of their stool, which is that DPR learned, I think it's in the spring of 2013, that law enforcement was investigating Silk Road and attempting to identify DPR. And then on -- was it on the laptop?

MR. TURNER: Yes, your Honor.

THE COURT: On the Ross Ulbricht laptop?

MR. TURNER: Yes.

THE COURT: All right. There was -- do you want that part? Maybe you don't want that part.

MR. DRATEL: Which?

THE COURT: The Ross Ulbricht laptop.

MR. DRATEL: You could say it was found on the laptop. That is good. That is where it was found.

THE COURT: On the Ross Ulbricht laptop there was a document, you can even say a multipage document. And then how would this be characterized setting forth various --

MR. TURNER: Titled "LE counterintel." In other words, "law enforcement counterintelligence."

THE COURT: Which the parties agree means "law enforcement counterintelligence." This document purports to contain a variety of information relating to ongoing law enforcement efforts with respect to Silk Road and DPR.

I think from that, then, Mr. Dratel, you can argue DPR

was on notice as of the spring of 2013. He had indications as to what he thought law enforcement was doing. You can't get it in for the truth, anyway, as to what law enforcement was in fact doing because that would be the hearsay purpose. And you can say it was a multipage document.

MR. DRATEL: Yes. Can I just --

THE COURT: Think about it?

MR. DRATEL: Yes.

THE COURT: Do you want to see my notes?

MR. DRATEL: I have it. The one change I would make is instead of saying "purported," the document does what does, so I would say that it is a document that contains communications to DPR about, then you could say purported criminal investigations or things like that. It is the "purported." I just think the communications are there. They are not purported.

THE COURT: Communications to DPR about a purported variety?

MR. DRATEL: Yes.

MR. TURNER: We would have no objection to that.

THE COURT: Let me just tell you sort of the three paragraphs I have so that is clear.

One. DPR learned in the spring of 2013 that law enforcement was investigating Silk Road and attempting to identify DPR.

Number two. On Ross Ulbricht's laptop there was a multipage document titled "LE Counterintel," which the parties agree means "Law Enforcement Counterintelligence."

Three. This document contains communications to DPR about a purported variety of information relating to ongoing law enforcement efforts with respect to Silk Road and DPR.

MR. TURNER: Maybe a variety of information relating to purported.

MR. DRATEL: That is fine.

THE COURT: A variety of information relating to purported ongoing. OK?

MR. DRATEL: Yes. I just want to go through the document to make sure it captures even in generic terms the full picture of it.

THE COURT: All right. Why don't you -- you've got the document. All right. But that would be the Court's, I think, way of trying to balance the defense interest in having those points but the government's interest in the potentially misleading impact of some of the way in which those are cast.

So let's see if our jurors are here so we can get started. But if I don't hear anything else from you, that would be -- and you can actually just read that as a stipulation, "The parties have agreed that."

MR. DRATEL: OK.

THE COURT: You don't have to -- obviously, that

witness wouldn't get this in.

MR. DRATEL: Right.

THE COURT: So she would then get in N and the Google stuff?

MR. DRATEL: Right.

THE COURT: All right. Terrific.

We are adjourned, and there was a mention of an issue that requires this portion of the transcript to be sealed, at least temporarily, until that is redacted.

All right. Thank you.

(Continued on next page)

/home/frosty/backup/project_references/le_counter_intel.txt

from East India Traitor on forum:

Well this obviously isn't private but i'll share jediknight is your attacker. I realize this will be treated like bullshit as most other info that gets relayed to you, but he is the script writer over at atlantis and brags of his assualt on your psuedo-revolution. I realize you support free market but even at the cost of attacks on your marketplace, you may say yes in public but i know this not to be true in your pirate head. Be sure to read my sig if this helps you otherwise
I want nothing more than for this to continue for as long as possible...soon the other markets will decentralize your profits and
vendors and you can retire...please do not let the dea follow your btc trails as they did in the past watchin your btc pile grow
daily until it was obvious who the owner of the mtgox account was...i know this is a non issue now but im just saying, they have
a quarter million dollar bounty on your head for info and have been here since May 2011.

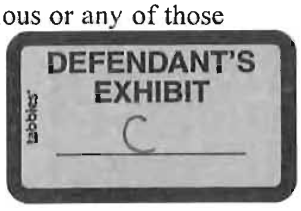
Attacker
SR Forum Profile: http://dkn255hz262ypmii.onion/index.php?action=profile;u=51427

Long story short I just did 6 months federal time in a DRAP program for SR related crimes,
currently living in halfway house very little time to get up to the local library to talk.
DEA visited/visits me twice a month...asks me shit, then they brag about their shit.
Such as the mt gox bullshit a couple months ago, asking if SR members would go for
paid informant work, I sent them on wild goose chases just enough to get them to
come share with me more than they could get from me. I in no way snitched out anyone,
they are currently trying to get into your staff forum mods esp...i suggest they change usernames every month start posts counts back at zero.
I suggest you relocate outside usa...if not already, they are foaming at the mouth which branch of the LE gets credit for your arrest.

blah blah got to run...last person in library have an 7:30pm curfew.
---
yeah it's more detailed
also covered that jediknight info was from an unlogged set of chat sessions so i dont have
links but the atlantis crew runs on the same server as the Silk Road IRC so to make a fake username and buddy up to them is no problem...the younger and smarter they are the more they brag. There's definately more details on the visits from the different visited me...esp trying to track down ovdb vendors and admin.

Please if there's something you have questions about ask and i will tell you what I know...they are pretty forthcoming and brag like any other ego driven personality. Like I said Im still on parole in a halfway house and visit a library to get
this back to you so my dedication to this is obviously a great risk to my freedom again except there is no way ill get a light 6 months federal
Residential Drug Abuse Program my second strike. So please understand I need this info I bring back to you and convey to
be Ultra Top Secret. Burned After Reading scenario.

Wow i never expected that.
Well let's start with the most important issue and I dont expect you to answer this to me but think,
"Who knows your real name in relation to Silk Road?" Admin from OVDB? Eneylsion or Envious or any of those guys?
What about people from the Bitcoin forums?



/home/frosty/backup/project_references/le_counter_intel.txt

"Do you have the servers in your name or a staff members name?" Hopefully these servers are spread out internationally.
Again these are rhetorical questions? I dont wanna know the answers just stuff for you to protect yourself.
Again the BTC block chain is definitely being watched for large transfers or deposit to same address which I assume was solved
long ago.
They know you have multiple btc tumblers and that you dont keep but around 1/3 of SR's btc balance on any given site.
Remember the agent that i spoke with that had been on the investigation started in late april 2011...i asked him and he told me.

The postal inspector asked me shit like why do i think you tell everyone to use USPS instead of private couriers and I told him
and he was pissed and wanted to know how I knew that. Then he wanted the postal workers that use SR in the forums real names..like I have a clue to that.
They expect shit that is unrealistic but I do know there's compromised vendor accounts and looking for the highest up vendors to interrogate.
They are paerticularly hung up on Limetless...they asked me about my money laundring and I of course said I have no idea how to do that cause admitting that gets you 15 years.
They seem to think Limetless laundrers for you, probably cause he has spoken about laundring in the forum opening countless times.
This isnt just a US investigation they ARE collaborating with other governments and international packages can be opened without a warrant. They simply have to have an address
on a postal list and it can be opened as part of the homeland security initative.

Sorry this is all I can cover today, I've go to spilt to get to a meeting at the halfway house...idk if i can hit the library on Friday but they let me go to there on Saturdays to "study law".
I'm trying to get some community service out of the way with the library as well so ill have more time here.

Thank you again and I'll be in touch very soon.

:)
---
ok not sure where we left off.
Let me explain my situation a little more.
See I still have contact with these agents, not in person anymore but by phone.
So guess who I talked to yesterday.
They are focusing on the forum and your admin and mods.
In particular Libertas and Samesamebutdifferent who is in my opinion your weakest link.
They dont really know anything about Libertas except he helps on the marketplace with coding...they have his tormail.
Idk what that does for them but they have ssbd's as well.
So i advise you to have them erase their emails and change tormail accounts or better yet not use tormail.
The way they got their tormail mail addresses is by importing their pgp ley and it was on there.
I have a feeling they think Libertas is scout...idk for sure but they have been asking about those three for months.
If by monday you can have them all start new usernames it is in your best interest as well as the community at large.

So you can see I have them in the perfect spot to play spy for Silk Road with the DEA.
Does this interest you?
Let's see what else...they believe that admin fromovdb is your chief code writer or at least the very least works on your staff.
They have envious' return address in montana some how.
They seem to think he might have some connection with you pre SR days...not sure why.

/home/frosty/backup/project_references/le_counter_intel.txt

Several agents question me on a fairly regular basis and are all doing different cases and sharing the info from interrogations.
I know there are things I'm not remembering at this very moment but when they do come to me I shall relay them to you.
If there is anything in particular you want to know if Ive heard about ask.
These guys vary in intelligence quite a bit from person to person...one cant use encryption another has been in the forum since it was on the orignal market.
They asked me if I knew anyone that bought shrooms from you and that if they had a return address for you...like that is even remotelty possible to come up with.
They are looking for every little think said in the forum about personal habits or the mods/admin..you.
Yesterday they told be they believed their was at least 2 ppl using the DPR username or more, which makes sense to me.
One for the forum bs and one for the marketplace.

Is this the type of stuff you are interested in?

As far as I know dont know anything about the shroom sales except you sold them sometime in the first month or couple months.
Mt Gox I was given anything but generalities...such as a huge amount of btc in one account that blew up in the matter of weeks, I'm thinking
they said around the time of the original gawker article...the public invite article.
They seem to be under pressure to get someone of great impoertance toshow a win for the USA on this situation.
And from what i gathered from the dea they were [issed they couldnt login during the dos attacks, so that says they had nothing to do wirth it, like i said anyway
jediknight was in chat bragging about how he had implemented escrow on atlantis in a 24 hour period and that he had plans to divert members from Silk road to Atlantis.
It wouldnt hurt i suspect to have someone look into logging chat on the atlantis channel that ios also non the SR IRC.

O just as i was about to sign out i remembered they asked me if Graham Greene was possibly a moderator or Admin.
I remembewr graham from before the arrest but ive been out of the loop for a couple of months so I really have no idea how much
he got involved in the forum...I know he was one of the more outspoken members that had the best interests of the community in mind
but i told them i didnt know that name.
---
can you give me links to where he is bragging?

what do you know about an mtgox account?

the DEA has a $250k bounty on me? how do you know?

==========

Cause i just did 6 months federal time for your revolution and they bragged about their doings too much upon interrogations.
They would visit me twice a month trying to get info from me..i would lead them on wild goose chases.
Just enough to get more out of them than they me.
They asked about offering the average member this bounty, how many would flip on you ,
they assumed 80% of the members would flip on you, but i know much better your following than them.
I also know that your current members dont have jack on you...but they are trying to talk to nelson you remember nelson right
from database days. He's still locked up.

I will also warn you that your staff is currently being targeted if not already a compromised one. Specifically the forum

members.

They followed an mtgox account that was in excess of some outrageous number of bitcoins, an account that should have had enough
bitcoin to be it's own exchange. They did not release the account username but they are very much obtaining info in manner
possible. I'm trying to warn you. The DEA, ICE, POSTAL INSPECTOR, NSI,FBI,CIA,NSA are itching to get credit for your arrest.

I advise you to relocate yourself from the US and before that have your complete staff change usernames at least once a month and no rolling over posts.

As far as jediknight i do not log chats so I cant link you to anything but that doesnt change the fact.

Like I said I just got back out and am on parole...so to clear up the info i have on jediknight it is at least 6 months old. But he was your denial of service instigator before the members started dos themselves and he and the atlantis crew are your troublemakers
as Im sure you've come to the conclusion yourself. I know without the exact quotes this is meaningless to you but at least I tried to make you
aware of the issues you are currently being annoyed with...and could even become your fall from grace.

Please delete all info as it is for your safety not mine. I want nothing from you and I am not trying to throw psyops at you. I've not always liked the way you ran the community
but I'm no traitor. I respect your progress on this frontier but I worry about your future. Along with the members futures.

If you don't believe me and wanna live in denial go ahead one day you will look back and wished you'd looked further in the rabbit hole.

---

scout's tormail where he is talking to mrwonderul:
username: scoutsr
password: b3l1am0n

Symm's tormail talking to mrwonderful:
symmetry2
bjBTrmPzUBhmN3uH

scout, forum
username: scout
pass: nlNlaGKUb1r6sqYY

StExo has discovered that Dr David DÃ©cary-HÃ©tu is planning to do research on SR for canadian LE
Address: Montreal, Canada
http://ca.linkedin.com/pub/david-d%C3%A9cary-h%C3%A9tu/41/298/702
http://jrc.sagepub.com/content/early/2011/09/20/0022427811420876

/home/frosty/backup/project_references/le_counter_intel.txt

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2119235
E-mail: david.decary-hetu@umontreal.ca

correspondence with alpacino:
silkpirate@tormail.org

This is for YOU only.

Try this (and I'll explain later why). Message your staff/moderators individually and ask "So, feeling wonderful lately? " and then ask "Anything you want to tell me?" Make sure to use the word "wonderful".

Theres an ongoing effort to engage and coerce your staff into giving up some access/insight/internal communications. Last I hear there IS headway on that. The key points are potential greed or intimidation. I believe it was someone @ DHS or CBP who wanted to own it, but ultimately its a DEA gig with a few cooks in the kitchen. Will absolutely request you not ever let on about this, and I'm sure you know how to run your team (and what level of trust to repose), but just know that absolutely there's an ongoing dialogue there with a "mr wonderful". Shocking, huh? Be smart about that.

Know that some of your vendors have been approached for (and have provided for money) buyer information (the idea is to purchase buyer information, which gets dumped and collated into excel). Vendors that get banned are approached via the email addresses they provide on their pages "in the event SR is down, contact here..". Just recently a New York based pill guy sold his entire customer list to what he thought was atlantis. Can find out his handle so you can poke around old private messages if need be. Several uses for databases of buyer information..

Am certain there are not many techies involved. Due to the unconventional nature of this network and technology, not much use for full time "geeks" being sourced & assigned anything more then standard workload. Unless there's some specific technical question/explanation needed

There are a few different working "profiles" on you (can probably get into detail later on how thats culled). The most popular is that you're East Coast , live with family, have either quit your office job or primarily do consulting/contract work from home. Theres other stuff I'd rather not get into, but rest assured anything worthwhile/concrete usually makes the rounds as gossip, and there's no real gossip. If that makes any sense..

There are really tons of useful nuggets that I do have to offer. And what my birdie doesn't know, he can probably find out, but no guarantees on timeframe. Due to the nature of keeping everything properly 'insulated', birdie has to fetch information with proper care. Also please realize the risk I run (and have run)..

Anything you want to ask?

I don't mind you talking my ear off asking questions.. there's a decent amount in my head, and fairly regular amount of chatter that makes it rounds to my ears. But as said, weekends are not optimum for me to poke my nose around as you can imagine the nature of this stuff (despite me being pretty insulated).. being casually brought up with the birdie(s) in anything other then a casual environment could trigger a disastrous chain of events for me. Evenings and weekends are probably when I can be more responsive.

1) That I struggled with myself, and anticipated. Well, I suppose you have no solid way of knowing. But ponder this - I have NO intention of asking YOU anything what so ever. There is not a single thing I have any intention or need to ask you. If this was a play to extract information/data out of you, it would be futile as there is not a single thing I want to know. If you dig around your staff's correspondence (unless already deleted) you will notice I'm right on the money

about "mr wonderful".I would not be privy to such if I was Joe Blow from nowhere. I can also tell you that one of your guys claimed he's been "recycled". That is the *exact* word. I am not sure if thats some internal term or it means he/she was in a different role and put into another one. I can assume it means a moderator or administrator was shifted from a previous role to a similar role. If that term "recycled" means anything to you, then that should at least speak to my legtimacy. Again, you do not have to acknowledge you know what that means. If it makes sense to you, then so be it, and if it doesn't then I can poke around more. I'm confident if you re-examine your staffs behavior and correspondence, it should verify my solid info. I'm not psychic, I'm not on your staff, therefore&

2)If you can come up with a method to verify I'm not, I am open to it as long as I'm able to protect myself to the fullest. I'm hesitant to touch any data, but I can (and do) commit things to memory.
There would be no gain in feeding you false information or lying to you. It would not benefit you in any way and you would realize your time is being wasted and that would be all she wrote. I think you are intelligent enough to parse bullshit from fact. Feeding false information would be the goal of someone intent on disrupting your activities or hoodwinking you. Again, something you would probably be able to verify - maybe half a year ago a guy from podunk Virginia contacted local and was crying about being blackmailed for his personal information by 'anonymous criminals' (Phil something). Middle aged guy who ran a travel agency. Even down to that level pops up on the radar nearby to where the birdie hangs out. Did not take long to assemble the backstory (small time recreational buyer just got blackmailed if you want to call it that by a crooked vendor) and dismiss as utterly irrelevant. I'm sure old private messages or communications can be examined to verify that instance.
How on *earth* would I be privy to that? And to know hard details? These things make the rounds, believe me. I would only provide you with things that could be of utility.

3) In short I admire you and what you've created, I don't think for a minute that helping you out time to time would hurt anyone (might sound hypocritical but it's not), and personal gain.
I don't think you've done anything that warrants resources of the state being delegated to interfere. I call a spade a spade, and JTFs/reports/operational/mindset are all a crock. I don't see anything wrong in what goes on here, and in another less boring life I'd probably have wished I could have been apart of it. Granted I'm technically on the other 'side' on paper (indirectly), but that's a means to eat. I'm not Snowden by any stretch, but I admire that. I've always tossed around the idea that how cool would it be if someone like the birdie would hook you up here and there, but the horror of getting utterly fucked and have my freedom taken would kill any such thoughts. But as I've said.. without being arrogant I know I'm relatively insulated enough by virtue of NOT being that close anymore. I'm a fly on the wall in the grand scheme of things. And more importantly, personal gain. If you're in a position to potentially augment your means & income, wouldn't you? I make a decent living, but I also have responsibilities and material desires. My conscience is clear because I don't feel I'm harming a single living creature. I don't come for free, so theres that motivation.

Worst case scenario I can provide you with insight and philosophy. Best case I can provide you with solid action-items that would unequivically give you a competitive edge.

I'm not trying to sell my utility to you, I'm pretty sure thats a no brainer. But I do think I can deliver..

I think that works. Initial+ weekly. I'm not entirely sure myself on what's fair or not fair.

Initial retainer.. I don't know, 5k too much or is 8k too much? I'll let you decide.
Weekly do you want to do 500? Obviously some weeks there will be nothing major other then chatter, and other weeks there might be extremely useful intel. I think we can just leave it at 500/weekly.

I made an account on your main site: "albertpacino".

Another thing, what I'm doing, despite all precautions (I've thought out all scenarios) could possibly ruin mine and my

family's life if ever discovered. I implore that never utter a word to a soul, a partner, a significant other, even God (if you're religious). I know you take security seriously, and you've demonstrated that, so I know you know where I'm coming from..
And if either of us ever wants to cease communication, then that should be an option and understood as a logistical decision, with no hard feelings.

Let's operate under your terms, and I will get to work tonight on writing up as much as I can RE you'r questions, then you can dissect and pick my brain with followups, then I respond etc.
I just have to be careful to walk a fine line that won't identify me or my location, but I've made a decision and I'm fairly confident in my abilities to satisfy your purposes and cover my ass too.

The only condition I have is that nothing I ever say be used in a manner that can harm anyones safety. Even if actual information is provided for some purposes (a vendor name or location), I would hope that nobody's safety is ever seriously jeopardized. Could not live with that. What you do with information (if involves threatening or anything) is your business, but nobody can actually be harmed.
I don't think you operate that way anyways..

I do have to run to dinner, so will get you get a comprehensive writeup later tonight.

And I do respect what SR stands for. In another life I'd have loved to be part of it. Maybe this is one way to live that fantasy out.

I know that Eileen has a publishing deal and is writing a book around SR, and has had extensive dialogue with everyone from buyers to new vendors to old hats. She claims that she has your blessing and at some point will be (or has) interviewing you of sorts. Also you've made reference to a book or memoir at some point. No matter what, I will make a gentleman's request that a word of this isn't spoken in this lifetime. I've taken many risks and gambles in my life and mostly have been lucky.. but the magnitude of what I'm doing, if uncovered, could put my family in harms way and/or devastate them and no money in the world could justify that. So that's that.

(Some stuff might jump allover the place as it comes to me, so apologies if theres more stream-of-thought and less organization)

Byt virtue of the professional capacity of a birdie I know, I have/had access and in-office/out of office knowledge of local, state and federal initiatives that deal with work tasked to monitor, report on, and coordinate interagency initiatives dealing with

1) Domestic movement of narcotics
2) Movement of narcotics traffic through land/sea/air borders
3) Cyber crime (extortion, child porn, domestic terrorism, credit card fraud, SPAM, password trafficking, counterfeiting of currency, computer intrusion, etc)
4) Financial crimes related to narcotics trafficking/distribution,/profit laundering

Prominent on the radar is Silk Road (amongst other known sites/actors on TOR) and since late 2011 there's been a lackluster yet interagency effort to monitor, disrupt, infiltrate and/or penetrate operations.
The office of the DAAG (Deputy Assistant Attorney General) Computer Crime (at time Jason Weinstein) was the principal in spearheading. This is after Sen. Schumer & party created a hoo-ha. Weinsteins office jumped to take charge and assume oversight.
Under the auspices of the NCIJTF (National Cyber Investigative Joint Task Force which is DOJ), the following fed agencies have a presence when it comes to SR (Stateside)
1) DEA

2) FBI
3) DHS
4) ICE
5) USPIS
6) ATF
7) CBP

That should NOT worry you, because by "presence" I only mean their are active agents and officer level involvement from who's resources are pooled and budgets are shared. On a limb I'll say this, everything having to do with Silk Road (like any other open set of investigations) is on shared drives that almost all can read+write, and there is a shared public Outlook folder where all emails/correspondence pertaining to SR are routed. Everybody (and I mean everybody) from entry level up to the heavens have "read" access. Additionally, people talk a LOT. Loose lips is an understatement and the level of immaturity and juvenile attitude is staggering. There is no such thing as "confidential", and this is a culture where people are numb. You must understand that part of why I'm so confident (in my ability to maintain this relationship) is that nothing is treated as sacred and there are probably 100 people like me who could offer the same level of access. Analysts do collate data and prepare summarizations/status sheets and CC the requisite list/group.. and majority of the time nothing happens. Little to none replies/discussion. This is not SR specific, but does include SR. For example reports related to CP sites/forums or BMR often get the same treatment.. ambivalence. Here is something that will bring a smile to your face.. it is just not in the budgets to aggressively dedicate resources to SR. The way the budgets are allocated are almost certainly political in nature, and the lions share goes to War on Terrorism or "real world" drug activity. That's the cold hard truth. That's not to say that there are no zealots who do have a harden for SR related activity, but that is more focused on suspected real world trafficking. Ironically enough, guys at USPIS do not care in the least about SR. Yes you read that right. They're broke and have no concept of tech savvy.. and frankly, they are not interested. DEA guys often initiate most chatter having to do with SR, yet follow up is minimum and they are too bogged down in pending investigations of subjects whom they have the ability to surveil and/or who's circle they can infiltrate by way of CI's (conf informants).. none of which is possible when dealing with a beast that is virtually immune to real world surveillance. It's not a question of getting warrants to ISPs.. its a question of who/where to begin looking. They're stuck.

At the analyst level, SR forums and the main site are crawled/monitored. Not more then 4 people are tasked with just crawling and mining the forums main site in an observational capacity. These 4 people are also tasked with crawling and mining many other websites and forums on TOR and clear net. So while everything is printed, you can guesstimate the scrutinity level is not extraordinary. That's not to say that others do not actively surf the forums and maintain both buyer and vendor accounts on the main site, they do. But at any given time, there are not more then a handful of people overseeing a crawl. When something deemed highly interesting or important pops up, they will CC the SR mailing list with a description and screenshot with their thoughts. Otherwise, there is a weekly status sheet that gets dumped with the most relevant/interesting/useful occurrences on the forum along with a summary on value/suggested "action items". Everything you post (along with the time stamps) is copied. You are referred to as DPR across the board. Often there is nothing interesting, and if there is there is it would be a bullet point such as "Vendor XYZ (who deals in ABC..) said his packaging methods consist of 123" etc. This is so they seem like they're doing their job as often there is nothing interesting at all taking place on the forum side. When moderators quote you, that is often the bulk of what gets bullet pointed "DPR has instructed us to do such and such".
Now, there have and continue to be attempts to compromise staff accounts (on the forum and main side) by the normal methods of password guessing, but AFAIK none have been successful. There have been successful instances of cloning lookalike accounts which have all been shut down on your side. Of significant focus is attempts to impersonate you and your moderators on not only SR mainsite/forum, but on other TOR sites such as BMR or Atlantis to see if any prior correspondences can be restarted. Nothing there either.

A 'profile' is an outline of a user that contains key points/occurences/assesment regarding their activities. There is not one on every single vendor, but there are on the high volume ones. The goal is to have all user profiles searchable offsite. In vendor profiles are return addresess/packaging method/pictures of the package & contents, replication of their vendor page text, and any other relevant data.
Your profile (no idea who authored) has you as extremely intelligent with a background in IT, between 35 and 55, living on the East Coast, working from home in a contractor/consulting arrangement and living with family. An

assessment like this would be based on your speech, patterns (such as when you log on, when you go idle on the forums), personality,expressed interests, ideology, unique mannerisms (for example your use of the word "ya" instead of "you" sometimes. As in "I'll tell ya" or "would ya believe" .. etc off the top of my head). The assumption is that you are conscious to actively remain off any kind of radar, do not take any drugs, do not live extravagantly.

If you have any partners (I'm not talking about staff), you most certainly are the assumed shot caller and are as anonymous to them as you are to everyone else. Contrary to rumors, it's not stated or assumed that you are not the original brainchild of SR or have ever not been the same person. You are the same you that started the site and have never relinquished ownership. Whether it's all you or you've farmed out responsibilities, it's unclear if the servers are all located in your physical possession or spread out. It's pretty much agreed that you have never been a vendor on the site or tied to any vendor IRL.
You're essentially a ghost. And since you are not a vendor, there is no tangible way to engage you in any compromising scenario. There have been attempts to approach you (can assume under the guise of journalists or researchers) to probably build a repertoire and study your speech, to later on analyze and compare if by some fluke there are any suspected leads on who you are IRL. As of now, I can say with utmost surety there are absolutely none whatsoever. You are as anonymous as you were 1 year ago. There HAVE been concentrated efforts to DoS/DdoS the site and forum to assess your response time and technical acumen. I'm not too savvy regarding this, but on a horizontal scope there have been/are attempts to run exit notes and track traffic across TOR. To what end this has been aimed at SR would be something I would need to poke around about.

Since the assumption is that security of the servers and high level system are handled solely by you, you are overworked and delegate lower level duties to your staff. There is a fixation on some how penetrating or compromising your moderators into giving access. The philosophy is that you are less stoic with your team and interact with them in a more informal fashion, which would provide insight into where you are located geographically and your habits (which could be identifiers). The Mr Wonderful operation (if you want to call it that) is still in progress and revolves around bribing or threatening your team into providing access to a staff account. The benefit would be to not only get closer to you, but to be in a position of trust in the community which could potentially net high volume vendors. A few of your staff have absolutely been in touch with Mr.W and most likely have carried on correspondence with them off-site. Mr. W is being actively maintained by DEA. Nothing major has come from this AFAIK, but tidbits have made the rounds such as there is fear of you and you have or had asked for personal information in the past in order to appoint members of staff. Also that you have "recycled" staff, which is taken to mean that either Cirrus is Scout (who has communicated with Mr W) and Liberatas could be Nomad Bloodbath. SSBD has also communicated with Mr.W. To what extent exactly the nature of their correspondences are, I do not know. I could find out, but it would not be immediate as it has to be handled with tact. If there was a successful breach of any staff account, it would be known and I would tell you. There has not been. Moderators are seen as loyal but weak, susceptible to intimidation and/or bribery. If their anonymity is ever compromised, they would turn. SSBD is assumed to be in the UK, where as Cirrus is assumed to be Midwest Stateside. Inigo UK, Liberatas States.
Assumption is that you also have employees on the main site who are completely unknown who handle maintenance and upkeep. No geographic assumption on any of them. AFA your relationship with vendors it is a rule of thumb that you do not have any special relationship with high volume vendors over other vendors. No vendor is assumed or perceived to be close to you. They will keep trying to open open lines of communication with you under various guises, even as vendors yet the likelihood of you befriending any vendor (real or agent) is nil. Locating you or the servers, although would be a major coup, seems all but impossible so the focus is aimed at netting vendors.

The high-vol vendor operations such as (to just name a few) Nod, NorCalKing, RxKing are all under scrutiny. They've all been purchased from multiple times and general geographic location is assembled. For example it would be known that the Nod operation is NY, NCK is in California, RxK is Southwest US etc. There are also ongoing attempts to befriend the 'biggish' vendors through private message/forum pm/privnote/pgp and take correspondence off-site. This is where off-site deals and 'partnerships' would get cooked up and layers of anonymity be peeled away, leading to more detailed profiles.
No high volume US vendor has been surveilled. On a state level, several suspected major vendors have been surveilled, yet none have been touched as that won't happen till a multi-jurisdiction plan to move on several vendors simultaneously in a grand slam display is logistically possible let alone greenlit. AFAIK, something of that magnitude

would not be possible currently. There have been one-off prosecutions on county and state levels. What happens is that a vendor that has confidently profiled/ascertained to be originating packages out of a certain jurisdiction, that information is shared down to local/state to put eyeballs on. A lot of that was happening in the beginning, but now there's more of a "hands off" approach. They'd want to sweep the maximum amount of vendors at once. Having the Sheriff of Mayberry hit one based on JTF intel is just not the culture/mindset. Nearly all efforts are conducted out of Jersey and Los Angeles.

All LE case reports (from county-level upwards) are indexed by a Lexus-nexus type database and can be searched for keywords. When they hit, they will hit several big vendors at once. They will parade them in front of the media and give the impression that the entire SR infrastructure was brought down (a la Farmers Market). Barring any unforeseen circumstances, there is nothing cooking at that level currently. Something of that magnitude would be seen coming well in advance and chatter would ramp up. There has never been heightened activity of that level in my birdie's time being a fly on the wall.

Posing as vendors - yes. That has happened. Although, DOJ attorneys will never ever allow drugs to 'walk' en masse. Especially after scandals such as Fast and Furious where the guns were allowed to walk.. they simply can not introduce narcotics into circulation. Vendor accounts have been bought to gain access to that side of the site and Vendor Roundtable and to establish longterm credibility, but any "purchases" would be absolutely fake and bought by their own accounts to build credible stats. I'm sure on state level there have been targeted vendor-posed operations to net bulk buyers, but those are highly controlled and short term. I have not heard of any of the top of my head. That does NOT mean that is not currently happening or will not happen in the future, but any significant bust would have made waves.

Vendors HAVE been approached off-site (most list their tormails on their pages) for customer information. This has been bought. Then collected and dumped. It has mostly been vendors who have vanished/been banned/ or slowed down. They're deemed to be the most vulnerable. This is not pursued as much due to a poor ROI. Most vendors/former vendors have not entertained such advances and those who have have demanded funds that simply are not available even in the discretitionary account(s). Like any other government effort/agency/JTF, funds are near impossible to get approved & released. Even undercover buys require paperwork and approval. There is no joint kitty of BTC available to make purchases from every vendor. It would take 2-3 days to get funds released for anything, and approvals are not that easy to obtain AFAIK. And in any case in this scenario, verifying information would be a nightmare. No guarantee that they would not just copy and paste names from the phonebook or use a name generating site. No real benefit other then to identify potential bulk buyers who would resell IRL (and this information would get kicked down to state/local).

Right now, there is a "watch and see" enviroment. I don't want to say that idea is to turn a blind eye by any means.. but until they swoop in to hit several vendors at once, there is no big fish in the cross hairs. The servers are a mystery, as is the leadership. Going after buyers would do absolutely nothing and not justify the budgets. Going after vendors one at a time also won't sit well as those get kicked down the food chain. Going after several vendors at once will be the play, bet on that. That will require compromising and turning CI's in each vendor's operation or periphery, which is not easy. Also, sustaining a DDoS against SR will not be the play either, I know this for a fact. Let me put it simple terms. You're winning. They just don't know how to tackle this beast effectively.

In all honesty I've had a very long day.. I'm kind of pooped right now. I'll have to call it a night. I know you'll have questions and I'll have answers and so on/so forth. Will hit the bed as I'll have probably have a fresher mind in the morning. Let's call it a night for right now.

I can only imagine. And usually the weakest link is the human element. We are all human, and all the precautions in the world don't mean a hill of beans if a slip up is made IRL. I don't want to give you a false sense of security, but you have done a thorough job of flying under the radar.

/home/frosty/backup/project_references/le_counter_intel.txt

One thing to be cognizant of, there's a lean on the domestic BTC exchanges to cooperate. There have been informal discussions in the last few months to develop working relationship with Coinbase (I know for a fact). After DHS hit Gox, even the boogeyman of a FinCEN violation is enough to mortify any of the btc guys. Anyone moving large sums of BTC will be open to scrutiny. I reference Coinbase because I know there was a series of meetings with Compliance at Coinbase. That can only mean one thing& BUT, that does not mean that the full on arm twisting by Treasury is going to be utilized to track black market vendors. They're more concerned (and justify) their desire for access due to terrorism. Most of the black market economy is essentially low hanging fruit in comparison to terror funding. But if OC activity is disrupted and theres political mileage for DoJ, the wide dragnet serves a multi faceted purpose.

1)
a) BMR is on the radar and that is ATF's baby. Politics plays a significant role in prioritization of which agency gets to own which investigations. The climate is aggressive when it comes to weapons trafficking and with the gun control hot potato has guaranteed virtually a carte blanche to ATF. And they have deep pockets as well. Because tor based weapons traffickers are almost always running guns IRL, there is synergy between federal and state. Federal approves staggering sums of money for surveillance,undercover and CI's. I don't want to say BMR is "infiltrated", but there are a lot of compromised accounts and there have been a few quiet busts. Nearly every bust has resulted in cooperation. I am not sure what the long play is, but as long as this current administration is in power the gunrunners will always be hard targets. They are intimidated with the threat of tangible charges (interstate trafficking, conspiracy, organized crime, distribution) and they ALL cooperate. The general consensus is that weapons dealers are not sophisticated and have a lot of IRL visibility, so they are ALWAYS on the radar.

"backopy" from BMR is also of significant interest because the operating assumption is that he maintains a healthy relationship with BMR vendors privately. This would have come from multiple compromised/cooperative vendors sharing their correspondence. He's thought to be a 1 man operation who's around the Las Vegas area. As to where the servers are is an unknown. The administrative structure of BMR is loosely unknown. But he's been a direct POC for cooperators and nothing I've seen or heard suggests that there are any hard leads on his location or identity. I do know that BMR/backopy is seen as a ragtag operation.

"East Coast Trade" from BMR has been discussed as a potential major middleman based on buys that have been made. This would stem from primarily quality of product and similarity to product that was interdicted at the street level.

b)HardCandy/Jailbaits are notably on the radar as they've been publicized in the media. Although these sites (and dozens other CP directories/forums) are on a permanent back burner when it comes to federal muscle. The consensus is that the hosting, content and major trafficking is foreign, so efforts should be coordinated under Interpol's umbrella. This is low priority.

c) HackBB and TCF are prominent and actively surveilled. Have not heard of any significant operations that have netted any majors, but there have been some successful prosecutions/interagency wins. HackBB especially is monitored closely. There is another counterfeit site whose name escapes me now, but there was a major sting that happened in Boston last winter which was a result of efforts focused on it. Paypal was involved and was very accommodating to SS in handing over logs.

d) Atlantis is too new to be taken seriously yet. It is not a honeypot.. it is for real. But it is being monitored and buys have been conducted. They're still figuring out where it stands and if it is fly-by-night or making a play to enroach into SR's territory. It is too early to tell and there is not significant traffic enough to justify re-allocation of resources.

2) Essentially yes. I have 'Read' permissions and can view docs.

3) Yes, a lot of people including my birdie are CC'd and have access to that email folder.

4) Both. Automated scripts primarily, and manually to a lesser extent. There have also been external (civilian) efforts to smart-crawl the site in a research capacity.

5) No. There has never been any names, concrete geography, or associations. Something like that would be a big deal, and not the kind of thing that would be able to be kept mum even if it was field-level. You are too "big of a fish" for it to be able to remain on the field. That is not to say that if the full resources of the state are at their disposal that they wouldn't be able to close in. But THAT is never going to happen. You aren't Bin laden, and there is not much political mileage in justifying millions in someone that is not physically trafficking in anything. You are operating a continued criminal enterprise and violating a host of laws.. sure, but you aren't moving drugs. You are not packaging and trafficking drugs. The irony is that although this is your show, the cast is more important to target. That is not to say that you shouldn't take precautions and your security very seriously. This entire Snowden fiasco has shed some light on what kind of impressive technology is at their disposal. Anybody can be surveilled at any point and wide enough parameters can be set to pickup on even the slightest unique identifier.. but again I can't stress enough, it's not in the budgets. If the spooks ever wanted to find you, that could happen.. but they do not and will not. There are no hard or soft leads on you, and I can swear on my children to that. If there ever were, I'd know about it.. and as per our arrangement, you would. But if you continue your SOP's in regards to security, you are a ghost.
It is believed that you are the same you since the beginning, and that ownership/administration has never changed hands. But you can sleep knowing that you are as known today as you were 2 years ago.. unknown. The door will not be kicked in just like that. There will be a flurry of activity for weeks and months beforehand.. a flurry that no birdie would be able to not notice.
Don't take that to mean you shouldn't have several outs and exits, which I'm sure you do. This is not my place to say this, but if I can venture some advice. Walk away from this one day. You've done something remarkable that will go down in the history books. But you are human, and humans are prone to mistakes. Any kind of mistake in your position would be catastrophic.

6) Yes. I can poke around more, but in short - yes. What the end-goal was, I'm not sure. What they assessed, I'm not sure. But further attempts on the integrity of the site will be executed, be sure of that. Although I can tell you, that won't be a long term play. It can't be sustained forever.

7) Not AFAIK. I can poke around and get back on this. But does not ring any alarms in my head. I vaguely recall some back and forth about a paper that was published, but I don't recall anything coming of it. This would be something on the tech side. I will circle back with you on this.

8) Some, yes. Off the top of my head - I know that "Costco" is a West Coast operation and theres some fair certainty that it's an Asian gang deal. There is an immigration element and tied to IRL dealing. I'm not sure what the wait is, but there's some play that probably involves state/local.
"Marlostansfield" is NYC, and the guy has a lengthy record and has been a CI in the past.
"Godofall" is NYC and they're Dominicans who are street level/wholesalers.
"DaRuthless1" has been surveilled by local in Queens and has a prior for distribution oxy.
"UndergroundSyndicate" I know was assumed to have been made, but there was some snafu with that and bickering state level.
I know there were a few California based pot guys who were being surveilled, I can circle back on vendor information. There is a vendor in Dade County, FL that was surveilled, grabbed and turned but the focus was on his IRL connects to coke wholesalers, not on mail.

I can poke around in regards to more on this topic.

I'm sorry if I said anything that makes you unhappy.. I would not lie to you about anything, I would not gain anything from withholding, rather you'd lose your utility for me and obviously that's counter to me even reaching out.

Please understand that it's obviously possible that I'm not privy to EVERYTHING that goes on. I work in a 9-5 environment and I'm nowhere near the field (and I'd never be). If there's something that you're 99.9% sure of is in

DPR's profile then you'd know better. If I don't know about it or have not heard/seen it, then that's a limitation of what I'm privy too. And I apologize for that sincerely, but I have no control over that.

As for #6, I can stress again that I'm not a technical person. From everything I've heard, it was the guys behind the DDoS. Thats the water cooler buzz so to speak. I said I have no idea what the goal was, if any. It's not my place to venture any opinions, but if someone else claimed to take responsibility then either they wanted to jump on the bandwagon, or they could have been trying to engage you and solicit some response. I am simply not consulted on operations.. I don't know any other way to put it. I'm a cog, not anything more.

I can stand by the profile of you that I provided. If there is more then I do not doubt it in the least, but it must be pegged as need-to-know.

RE your scenarios - I reached out to you for, as I said, personal gain. There is no card being played.. believe me I'm not in the game. To placate you into a false sense of security.. but then ask for compensation? That doesn't make sense. I see what you're saying, and I don't blame you, but if that scenario had any merit, why would I "compromise" the Wonderful deal? Do you see what I'm saying?
Scenario 2 is one that I'm whole heartedly (well, heavy heartedly) willing to accept. I do concede that I'm not an agent, I'm not operational, I'm not field. I'm a worker bee and I do feel I'm useful.. and I'm willing to prove it (while also covering my own ass). But if you feel I'm not as useful as you had hoped.. I'm pretty damned sorry and I can accept that?

I'm open to whatever you suggest..

Well now you have me thinking too.
It's one of two things:
Out of an abundance of caution. There could purposely be bogus OR outdated profiling (left over from a legacy report). Knowing theres various agency crosstalk (and curious eyeballs), the thinking can be to keep sensitive information off the shared drives for fear of someone going into business for themselves. The nature of btc and tor can tempt anyone to come to you (as I have) with something you'd presumptively write a blank check to get your hands on. Leaks happen all the time.. but generally they're to the press, not the subject. Could be a safeguard. Or, could simply be because your sources might be closer to the field and have first hand knowledge of updated working data.

The DDoS would certainly be NCIJTF/FBI. There would not need to be any full time geeks tasked with attacking or penetrating SR and nothing else. Could only be 2 ways:
1)They would assign a group internally, fast track the assignment approval, provide an objective and get briefed on any developments. This isn't open ended and there has to be some goal/metrics to be reported on in a specified timeframe.
2) Farmed out to a contractor. A lot security specialists are contracted out by the FBI. This is a bit murkier as they operate on their own guidelines and are just asked to deliver with minimum oversight.
But they have limited resources at their disposal unlike employees.

This is something I can dig around and find out if it was internal or outsourced. I can also find out if theres a set group that's been delegated specifically to SR. Would also be able to ascertain which office they'd be out of. Most importantly I can try to see what (if anything) has been the yield and what the priority level is. If I start getting too technical with my poking around that might raise a flag.. so it's a balancing act for me. But I can get you something RE: past IT based attacks on your infrastructure.

I will, that is something I can do that might shed some light on the attack(s). Engaging you/intake of your response is attempted by every means. This is my opinion, but even if it was legitimate extortion does not rule out a contractor(s) sourced by LE. Anybody can see dollar symbols and see a financial opportunity even if they've been tasked by feds. Now, if it was in-house then yes, demanding payment to ceasefire would be bizarre as there would be too much oversight on the operation and if you had gone public (for example) with the fact the attacker is asking for payment.. there'd be disciplinary action at the very LEAST. But you are right in the sense that highjacking/ransoming the site for profit is not how LE operates. I'm thinking if the attacker was not LE, then they launched a separate attack with the wishful thinking that the massive onslaught would disrupt the site long enough to cause hot vendors to go back on the streets and open themselves up to catch cases.
I will look into this.

There are a few shared drives, but the lions share of SR related data is dumped to a drive titled (I'm not being humorous) "Silk". I would say SR related maybe 3 gigs? As for getting a copy of it -
this is scary. I don't know how/when/IF such a thing would be audited. Do you know? I'll research. But the thought of making a copy of all the folders onto an external from my workstation.. that really turns my stomach. What if theres a system wide audit of who copied/moved/read/wrote what folders/files and it's asked of me what I was doing copying that entire folder to a USB..we're talking Do Not Pass Go, Do Not Collect $200, straight to prison. But maybe I'm being paranoid as well, because there are so many cooks in the kitchen and people move folders/files all the time. No cameras where any of the cubes are.. so theoretically if I found an open work station, a copy *might* be possible. But I can tell you that the risks involved in this are unquantifiable. I can think this one through. Maybe copy some docs at a time, in 2 or 3 passes. Let me read up on how/what can be audited.

Every avenue is being explored by Treasury and HSI (Homeland Sec Investigations) to get claws into the Bitcoins exchanges. By claws I mean sweet talk and then flat out intimidate.The view in LE circles is that Bitcoin exchanges are shamelessly serving as money launderers and know very well that a wide chunk of the bitcoin economy is from black market transactions. Now, when Gox was hit in the spring.. that was literally over an unchecked box on some form asking "Are you a money transmitter?"! Because (the US subsidiary) of Gox failed to check the "Yes" box.. that alone was enough to get a judge to sign off on a warrant. The rest is history. LE has reached out to EVERY SINGLE DOMESTIC btc exchange and asked them to share records on vague grounds (ongoing narco-traffic investigations, Islamic charities/donations etc) and establish channels. The exchanges seem to talk to each other, and have by large put a united front and rebuffed these advances so far and have insisted their Ts are crossed and I's are dotted, which means they are not obligated to share records with any LEA on gratis. And since their paperwork is in order, LE is stuck here. They have not been enable to find cause to hit any of the other exchanges the way they hit Gox. I can tell you that LE is so used to banks bending over backwards to accommodate, they're annoyed that the exchanges have not rolled over. They have not seized servers of any domestic btc exchange. Even Mutum Sigillum's seizure was just their Dwolla account, not their servers or any stateside Gox data. Coinbase, however, is probably playing ball at some level. If you recall they scored like $5mil in a Series A round a few months ago. Few weeks after that (I'm talking June), there were meetings between there Compliance/attorneys and Treasury. This is not public knowledge. Either this was the investors insisting that they reach out to the feds and get in their good graces, or Treasury tried to squeeze them and maybe found something they thought they could use to bully them. But that's been quiet since. Have not heard anything. Gut says they probably reached some tentative agreement to pass on records in a limited capacity. Long story short, no, they are not tapped in to the exchanges (yet), aside from possibly Coinbase.

Civilian leads come in all the time to both local and federal. Sometimes its a call to one of the tip lines, and sometimes from confidential informants on the local level who are helping build cases on street dealers, and the street dealers are suspected of putting drugs in the mail or fedex, and SR is mentioned. Other civilian leads would be from academic research regarding SR/TOR (crawlers, potential bugs/flaws in the tor network etc). Or then instances of someone coming to local LE for help because they were being extorted and 'threatened to have their information released allover SR forums" etc (usually a buyer that's getting blackmailed by a vendor) have also trickled in.

/home/frosty/backup/project_references/le_counter_intel.txt

Yes, I'm thinking slow dump to USB, then PGP'd and sent to a tormail you provide. Will have to be slow, and ideally any chance I get to an open machine that I'm not logged into. The good thing is people don't take their workstation security serious and are pretty lazy.

What are your thoughts on this RE the weeklies and anything that comes through the pipe on Outlook. I was considering screen shots, but then the fear of an audit catching an outrageous amount of screen shots might be a problem. So, suppose I got an old iPhone or anything with a high res camera, and pulled up docs and took pictures? Then can transfer the pics later, remove exif data, crop out anything identifiable (reflections, other open work on the machine) and then send? Although crude, this would at least work in terms of getting your eyes on stuff. Fallback would be you wouldn't be able to copy paste anything. Thoughts?

About Gox: No way. Hitting Mutum Sig was a last resort and reactionary because they had approached Gox directly and were rebuffed, and then reached out to the Japanese government to no avail. Although on good relations, Japanese companies are very anal when it comes to perceived threats to their bottom line. Must not forget that Gox is fully aware that that a staggering amount of traffic is dirty money (no offense), and that makes them money. They can't fathom turning over records and data to the Americans without a crippling mass exodus of capital (if it ever came to light). Also Japanese are a proud people when it comes to their work. There are free trade agreements with Japan that have binding clauses to provide financial information to requests from say the IRS, but something that like can't be used as a tool with the Japanese government because of limited resources and approvals on our end. It's very beauracratic and not just a matter of a few phone calls and emails. And even still the Japanese can stall and pushback. As long as Gox is operating where they are, they will guard the integrity of their records/logs/data. Gox is outside the tentacles.

No no, I can, I was thinking in terms of immediate data transmission. Grabbing off the drive is going to have to be done over some time. I can copy the contents of the weeklies to a file.. especially as they're sitting in Outlook. It does make my stomach turn.. but I know I've made a decision and opening emails is not out of the ordinary for me. I just have to remind myself that I'm as anonymous as can be and the financial incentive is attractive. And realistically I'm one of around 100 or more who would routinely be privy.. so I don't stick out. But Jesus this is scary. Sorry, just thinking out loud. I do appreciate you reposing trust in me and being generous with comp.

When I put my paranoia into perspective vis-a-vis what stress you must live under.. and see a (wo)man who's seemingly calm and collected, that does ease the burden. At the end of the day us corresponding on tor is as safe as can be. And my age/appearance is helpful in regards if ever asked why I'd be accessing SR specific docs/folders.. it's not entirely bizarre that I'd be curious in counter culture. And without getting into my position, I am tasked with a lot of gruntwork that involves being in various drives. Because of my clearance I haven't even done drugs in ages and can't.. so I've never indulged in the site. And this method of correspondence was thought out by me for weeks. I'm not on my personal machine. God forbid the day would ever come where an eyebrow would even be raised though.

I know you know how to keep an eye on your staff.. but realize that correspondence on the Wonderful situation is something you'd want to pay close attention too. Even if your guy(s) swear up and down the moon (to Mr. W) that you aren't in the know they've been talking, it will be assumed that you ARE watching and/or playing them directly. That can be a pro or a con for you, depending on how you finesse the situation. They either feed disinformation and/or take anything relayed with a grain of salt. I would not let your staff know you know they've been talking.. not only would that raise a flag, you'd lose a major opportunity to manipulate the situation. Bottom line is, assume they're

compromised or infiltrated, and you can have the boys running on goose chases.

The more you send confusing signals via the forum and manufacture events, probably the better. For example to post that you're satisfied with the new setup/configuration of the server would be a good throwoff/distraction. Or to let speculation run about how many people are DPR/has SR changes hands and whatnot is advantageous to you (but you knew that). Or even to appear to unconsciously reveal an identifier about your habits/intentions/origins is good psychological warfare (but you knew that too).

As far as your vendors go.. that's the weakest link. You have to keep an eye on their PM's and behavior/correspondence. Keeping them off the street, encouraging they partner up to appear to be operating out of various geography, monitoring their attempts to work outside the framework and open themselves to under covers are all no brainers but imperative.

I'm going to poke around all I can on previous attacks/future plans of assault on the site.Know that paralyzing the site forever would never be an end goal of LE. That would be anticlimactic. Breaching your site security would be, and if that were to happen, they'd sit on it and watch.. with no time constraints. And still target the high volume vendors. If that were too happen, it would eventually filter back to me and thus you, and how you tackle it is obviously your call.

If the climate in regards to the BTC exchanges changes and theres heightened interaction with Treasury/HSI, I will tell you the who and when. That might help you strategize big picture. For right now they're safe. That could change.

I assume you'll want to know of street level activity or buzz that comes in via local or USPI, even if mundane. I'll get that to you too. If I can't get a vendor name, I can provide you with the geography and whatever identifiers I find. But these guys are almost always flipped and used to setup their IRL connects.

Also, do not put it past them to wiretap journos. If you (for example), interact with people like Chen or Ornsby, assume they can see it. Assume journalists are compromised/breached.

What I'll do this week is figure out how to start gleaning docs off the drives, and copying the weeklies/emails. Will need a few days to get that sorted out. I do sincerely hope that all this helps/will help you.

I guess that wraps up our initial framework. I don't know anything else off the top of my head that might be critical. But if something does come to me then I'll inform you. Give me a tormail where I'd be able to send stuff to. I'll create one as well strictly for this purpose.

If I'm not missing anything.. then I assume the first part of our initial arrangement/deal is squared away? If you could take care of the balance of my retainer tonight I'll have some peace of mind that I'm starting the week/this chapter of my life squared away. And the weekly comp following the weekly data that comes your way? I assume that's fair?

Ok, got it. Thank you for that DPR, you're a man of your word as am I. Thank you for being receptive.
Most weeks there's something at least.. so "nothing new or interesting" is almost never the case unless theres a complete lull or resources are re-allocated to some pressing other business. Even if there's nothing "new" per se, I can always engage others informally and chat them up to see what the buzz is. I'll figure out the doc/files and send them encrypted to that address. Feel free to ask any questions whenever, I'll check this forum account every evening and again at night. During working hours is almost possible unless I'm working from home, in which case I'll be reachable. If there's any specific you'd want want me poke around, then just point me in the right direction and I can circle back. Sorting out what else they have that isn't in the current profile (and why/how it's omitted) as well as the what/who/where/why RE the DoS I've put on top priority. I'll get something.

```
<?php

class Support extends MY_Controller {

    public $message_limit = null;

    public function __construct() {
        parent::__construct();
        if ($this->userid != $this->admin && !in_array($this->userid, $this->
            support_admin) && $this->uri->segment(2) != 'landing' && $this->uri->
            segment(2) != 'login') {
            die('no access');
        }
        $this->message_limit = 70;
    }

    function all_images() {

        $items = $this->db
            ->select('items.image_id, items.id')
            ->from('items')
            ->join('users', 'users.id = items.user_id')
            ->where('items.image_id !=', '')
            ->where('items.quantity >', 0)
            ->where('items.stealth', 0)
            ->where('users.active', 1)
            ->where('users.stealth_mode', 0)
            ->where('users.role', 1)
            ->group_by('image_id')
            ->get()->result();

        foreach ($items as $item) {

            echo $this->extras->image($item->image_id, 2).br();
            echo $item->id.br(2);

        }

    }

    function landing() {

        if ($this->user_info->id) exit('already logged in');

        echo form_open('support/login');
        echo form_input('user');
        echo form_password('pass');
        echo form_submit('submit', 'go');
        echo form_close();

    }

    function login() {

        if ($this->user_info->id) exit('already logged in');
```

```
        $this->load->library('hasher');

        $pass = $this->input->post('pass');
        $username = $this->input->post('user');
        $user_id = $this->market_model->single_cell('users', 'id', 'user',
            $username);

        if ($user_id != $this->admin && !in_array($user_id, $this->support_admin)
            ) exit('no access');

        $user = $this->db->from('users')->where('id', $user_id)->get()->row();
        $db_pass = $user->pass;
        $usalt = $user->usalt;
        $hash_pass = $this->hasher->hash_pass($pass, $usalt);

        if ($db_pass == $hash_pass) {

            $this->ma_session->set_data('user_id', $user_id);
            $this->ma_session->set_data('token', rand());

            if ($user_id == $this->admin) redirect('mastermind');

            redirect('support');

        } else {

            exit('invalid login');

        }

    }

    function index() {

        $now = time();
        $one_month_ago = $now - 30*24*3600;
        $two_days_ago = $now - 2*24*3600;
        $three_days_ago = $now - 3*24*3600;
        $one_day_ago = $now - 24*3600;

        # customer support data
        $data['customer_message_count'] = $this->db
            ->from('messages')
            ->where('read', 0)
            ->where('to', $this->support_id)
            ->get()->num_rows();
        $customer_message_freshness = $this->db
            ->from('messages')
            ->where('read', 0)
            ->where('to', $this->support_id)
            ->order_by('created', 'asc')
            ->limit(1)
            ->get()->row()->created;
        $data['customer_message_freshness'] = $this->extras->display_freshness
            ($customer_message_freshness, 'short', 2);
        $data['cs_in_3d'] = $this->db
```

```
        ->from('messages')
        ->where('to', $this->support_id)
        ->where('created >', $three_days_ago)
        ->get()->num_rows();

    $data['cs_in_1d'] = $this->db
        ->select('from')
        ->from('messages')
        ->where('to', $this->support_id)
        ->where('created >', $one_day_ago)
        ->distinct()
        ->get()->num_rows();

    # vendor support data
    $data['vendor_message_count'] = $this->db
        ->select('from')
        ->from('messages')
        ->where('read', 0)
        ->where('to', $this->vendor_support_id)
        ->distinct()
        ->get()->num_rows();
    $vendor_message_freshness = $this->db
        ->from('messages')
        ->where('read', 0)
        ->where('to', $this->vendor_support_id)
        ->order_by('created', 'asc')
        ->get()->row()->created;
    $data['vendor_message_freshness'] = $this->extras->display_freshness
        ($vendor_message_freshness, 'short', 2);

    $data['vs_in_3d'] = $this->db
        ->select('from')
        ->from('messages')
        ->where('to', $this->vendor_support_id)
        ->where('created >', $three_days_ago)
        ->distinct()
        ->get()->num_rows();
    $data['vs_in_1d'] = $this->db
        ->select('from')
        ->from('messages')
        ->where('to', $this->vendor_support_id)
        ->where('created >', $one_day_ago)
        ->distinct()
        ->get()->num_rows();

    # resolution data
    $resolutions = $this->db
        ->from('transactions')
        ->where(
            array(
                'action' => 5,
                'finalized' => 0,
                'canceled' => 0
            )
        )
        ->order_by('created', 'desc')
```

```
            ->get()->result();

        $count = 0;
        $resolution_freshness = $now;
        foreach ($resolutions as $resolution) {
            $due = $resolution->dispute_opened + $resolution->dispute_duration;
            if ($now > $due) {
                $count++;
                if ($due < $resolution_freshness) $resolution_freshness = $due;
            }
        }
        $data['resolution_count'] = $count;
        if ($resolution_freshness < $now) $data['resolution_freshness'] = $this->
            extras->display_freshness($resolution_freshness, 'short', 2);
        $data['reso_out_3d'] = $this->db
            ->from('resolutions')
            ->where('proposer', "0")
            ->where('created >', $three_days_ago)
            ->count_all_results();
        $data['reso_out_1d'] = $this->db
            ->from('resolutions')
            ->where('proposer', "0")
            ->where('created >', $one_day_ago)
            ->count_all_results();

        $data['user_flags'] = ceil($this->db->query("SELECT SUM(weight) as w FROM
            flags WHERE type = 'user' GROUP BY type_id ORDER BY w DESC")->row()->
            w);
        $data['item_flags'] = ceil($this->db->query("SELECT SUM(weight) as w FROM
            flags WHERE type = 'item' GROUP BY type_id ORDER BY w DESC")->row()->
            w);

        $data['withdrawal_switch_state'] = ($this->extras->get_var
            ('withdrawal_switch') ? 'on' : 'off');

        $data['view'] = 'support/support';
        $this->load->view('support/template', $data);

    }

}

# end
```

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	14 Cr. 68 (KBF)
- against -	:	**NOTICE OF MOTION IN SUPPORT OF DEFENDANT ROSS ULBRICHT'S POST-TRIAL MOTIONS**
ROSS ULBRICHT,	:	
Defendant.	:	

PLEASE TAKE NOTICE, that upon the annexed Declaration of Joshua L. Dratel, Esq., and all prior papers and proceedings herein, the defendant, ROSS ULBRICHT, will move before the Honorable Katherine B. Forrest, United States District Judge for the Southern District of New York, at the United States Courthouse located at 500 Pearl Street, New York, at a time and date to be set by the Court, or as soon thereafter as counsel may be heard, for the following relief:

(a) an Order of a new trial, pursuant to Rule 33, Fed. R. Crim. P., based upon the government's failure to provide exculpatory material in a timely manner;

(b) an Order renewing Mr. Ulbricht's suppression motion(s) and granting them in their entirety and/or for a hearing on the suppression motion(s); and,

for any such other and further relief as to the Court seems just and proper.

Dated: New York, New York
6 March 2015

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

Attorneys for Defendant Ross Ulbricht

To: CLERK OF THE COURT

UNITED STATES ATTORNEY
SOUTHERN DISTRICT OF NEW YORK

ALL DEFENSE COUNSEL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	14 Cr. 68 (KBF)
- against -	:	
ROSS ULBRICHT,	:	
Defendant.	:	

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

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

EXHIBIT 1

Exhibit 1 to Ross Ulbricht's Rule 33, Fed.R.Crim.P., Motion for a New Trial

- 3505-14-22[1] – JDY[2] Affidavit 5/29/2013 for NDIll search of MK e-mail accounts;
- 3505-24-25 – JDY e-mail 05/05/13 re: suspicious Dwolla accounts;
- 3505-34 – JDY email 11/08/12 re: "username that DPR uses on several other sites[,]"[3] referring to AA.[4]
- 3505-205 – email 08/15/13 from AUSA ST[5] to JDY re: warrant application affidavit
- 3505-206-33 – JDY draft Affidavit 8/15/2013 for SDNY search of MK[6] e-mail accounts
- 3505-334-35 – AUSA ST Sealing Order application DATE re: "target of this investigation" (referring to MK)
- 3505-236-39 – JDY 10/12/2012 email re: subpoenas re: MK (German companies)
- 3505-250-51 – JDY 8/3/2012 email re: MK and Ashley Barr "running the Silk Road"
- 3505-265 – JDY 9/10/2012 email re: MLAT[7] to Germany
- 3505-267 – JDY 7/11/2012 email re: "We think we found out who's behind the SR."

---

[1] 3505 is the prefix designation for 3500 material for Homeland Security Investigations Special Agent Jared Der-Yeghiayan. 3501 is the prefix designation for 3500 material for Internal Revenue Service Special Agent Gary Alford.

[2] "JDY" refers to Homeland Security Investigations Special Agent Jare Der-Yeghiayan.

[3] "DPR" refers to "Dread Pirate Roberts."

[4] "AA" refers to Anand Athavale.

[5] "AUSA ST" refers to Assistant United States Attorney Serrin Turner.

[6] "MK" refers to Mark Karpeles.

[7] "MLAT" refers to Mutual Legal Assistance Treaty.

- 3505-273-75 – JDY 5/15/2013 email re: MK investigation and internecine law enforcement agency conflict, seizure of MK account, and criminal 1960 violations
- 3505-285-87 – JDY memo re: Operation Dime Store and MK "administering the Silk Road website with the assistance of multiple other associates."
- 3505-295-301 – JDY memo re: internecine law enforcement agency conflict and MK attorney meeting, etc.
- 3505-302-06 – JDY memo re: accounts controlled by JDY and others, including four pages of redactions
- 3505-315-16 – JDY email 11/13/2012 re: AA internet presence
- 3505-316-18 – JDY emails 11/13/2012 re: AA
- 3505-334 – JDY email 8/18/2013 re: MK and MediaWiki version 1.17.0
- 3505-355 – JDY email 9/16/2013 re: weird bitcoin movement in August 2013
- 3505-537 – JDY email 4/20/2012 re: "going right for the admin and his money. We have a few of the silk road's account numbers identified."
- 3505-539 – JDY email 4/18/2012 re: "We've identified a few of Silk Road's bitcoin account numbers and are working to further identify the people behind them."
- 3505-588-90 – JDY emails 11/13/2012 re: AA ("Vancouver target")
- 3505-591-600 – JDY November 2012 report re: AA
- 3505-626-28 – JDY emails 5/22/2013 re: AA investigation
- 3505-630 – JDY email 11/2/2012 re: AA & MK investigation re: DPR writings
- 3505-632 – JDY email 5/8/2013 re: MK and Mt. Gox/Dwolla accounts
- 3505-671 – JDY email 11/26/2013 re: MK the purchaser for silkroadmarket.org
- 3505-673 – JDY email 9/9/2013 re: German registry company records
- 3505-707 – JDY email 10/7/2013 re: MK "purging everything after his arrest . . ."

and GA[8] email re: hacking of bitcoin forum shortly after RU's arrest.

- 3505-709-10 – JDY email 7/12/2012 re: grand jury subpoena to PayPal re: MK activity
- 3505-712 – JDY email 7/16/2012 re: "I think we figured out who's behind the SR."
- 3505-735 – JDY email 2/27/2013 re: MK and German companies and servers.
- 3505-738-39 – JDY emails November 19, 2012 re: AA investigation
- 3505-775 – JDY emails 9/29/2013 re: "peaceloveharmony" "sitting on DPR's profile for a few hours."
- 3505-787 – JDY emails 8/2/2013 re: "inlightof" and "it's my opinion he was the previous DPR. Current DPR is new as of appx April we think."
- 3505-835-36 – JDY emails 1/15/2013 re: "should have an indictment and arrest warrant by the end of March." "I do have actual plans on doing something very large in the next month or so, . . ." "we're likely to see this site fall soon."
- 3505-846 – JDY email 11/13/2012 re: AA investigation
- 3505-895 – JDY email 10/15/2013 to AUSA ST re: Excel spreadsheet of "Karpeles Dwolla Transactions"
- 3505-00902-02916 – spreadsheet of MK's Dwolla transaction history
- 3505-2925 – JDY email with respect to Ross Ulbricht's Mt. Gox account(s), "just heard that information was passed from MK's atty's to Baltimore[,]" and that MK remained under investigation by HSI Chicago.
- 3505-2933 – JDY email 7/14/2013 re: "Cirrus is scout, insight of might be dread according to scout."
- 3505-2935-36 – GA email 9/17/2013 to AUSA ST re: Richard Bates and "[c]ould be worth looking into this guy . . ."
- 3505-2954 – JDY email 8/15/2013 to AUSA ST commenting, upon reading the interview of DPR in *Forbes*, "Yeah, it sounds very much like MK."

[8] "GA" refers to Internal Revenue Service Special Agent Gary Alford.

- 3505-2961 – JDY email 2/11/2014 re: bitcointalk.org administrators, including MK.
- 3505-2991-92 – JDY email 8/28/2012 re: interference from other agencies and jurisdictions
- 3505-3002 – JDY email 4/3/2013 re: "there has been a little movement from Vancouver on the suspect there."
- 3505-3006 – JDY email 4/10/2013 re: AA investigation
- 3505-3020 – JDY email 10/2/2013 re: "after reviewing some notes from [Mr. Ulbricht's] computer last night/this morning there appears to be some inferences to MK's involvement and associations to SR."[9]
- 3505-3045 – JDY email 7/17/2012 re: "[t]he main target (Mark Karpeles) has been in Japan I believe since 2009 . . ." and Ashley Barr and the investigation.
- 3505-3057-58 – JDY emails 4/3/2013 & 4/4/2013 re: investigation of AA
- 3505-3063-65 – JDY emails 5/23/2013 & 5/24/2013 re: AA investigation
- 3505-3068-85 – JDY report re: AA personal profile and language analysis
- 3505-3122-24 – JDY report re: "Agents have discovered strong ties between those controlling the bitcoin markets and those operating the Silk Road." "Over the last few months, HIS O'Hare has made several breakthroughs in identifying high priority targets believed to be the backbone of the website." "HSI O'Hare has also identified multiple financial accounts belonging to the Silk Road operators which contain bitcoins equal in value to millions of U.S. dollars."
- 3505-3086 – JDY email 4/16/2013 re: draft affidavit for search warrant for MK emails
- 3505-3087-92 – JDY draft search warrant affidavit for MK email accounts
- 3505-3447-50 – JDY email 10/12/2012 re: subpoena to API GmbH re: MK
- 3505-3472-74 – JDY email 7/11/2012 re: MLAT request to Germany re: MK
- 3505-3475-80 – JDY report re: investigation and MK

[9] "SR" refers to Silk Road.

- 3505-3512 – JDY email 9/30/2013 re: looking for connections to MK in DPR private messages
- 3505-3703-10 – JDY Report 36 08/06/12 re: MK investigation
- 3505-3722 – JDY Report 39 11/14/12 re: AA investigation with redactions, *including AA's name and identifying information*
- 3505-3762-67 – JDY Report 45 03/07/13 re: MK investigation (and redactions)
- 3505-3809-23 – JDY Report 54 05/01/13 re: AA investigation with redactions on information gathered by JDY regarding AA (3505-3817-23)
- 3505-3825 – JDY Report 55 05/06/13 re: missing paragraphs from Report 54 (but redacted)
- 3505-3869 – JDY Report 63 10/17/2013 re: search warrant served on Google for MK's email addresses
- 3505-3900-03 – JDY Report 75 11/27/2013 re: Customs Mutual Assistance Treaty request and return from Frankfurt, Germany re: MK (with redactions)
- 3501-43 – GA email 9/25/2013 to PayPal re: "the subject identified in the request we have reason to believe may work for eBay/Paypal or have a significant connection to your company."
- 3501-83 – GA report 10/12/2013 re: SR investigation noting "FBI tech specialist who said that the server did not reveal any identifying information as to the identity of DPR and was not the 'home run' that FBI was seeking."
- 3501-153 – GA emails 10/18/2013 to AUSA ST re: a bitcoin account related to "Justin's" account that was "emptied shortly at the end of July"
- 3501-157 – GA emails 10/16/2013 re: evidence that Mr. Ulbricht was a bitcoin trader for years
- 3501-206 – GA report 9/27/2013 re: "Interviews were obtained after the takedown of SR in various parts of the country by IRS and DEA counterparts upon the direction of SA Alford."

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

TO BE FILED UNDER SEAL

November 21, 2014

By E-mail
Hon. Katherine B. Forrest
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross William Ulbricht*, 14 Cr. 68 (KBF)

Dear Judge Forrest:

The Government writes respectfully concerning an ongoing federal grand jury investigation being conducted by the U.S. Attorney's Office for the Northern District of California ("USAO-San Francisco"), in conjunction with the Public Integrity Section of the Criminal Division of the Department of Justice. The subject of the grand jury investigation is a former Special Agent ("SA") with the Drug Enforcement Administration ("DEA"), named Carl Force. In 2012 and 2013, SA Force was involved as an undercover agent in an investigation of Silk Road conducted by the U.S. Attorney's Office for the District of Maryland ("USAO-Baltimore"). As the Court is aware, USAO-Baltimore has a pending indictment against Ross Ulbricht, charging Ulbricht with, among other things, soliciting the murder-for-hire of a Silk Road employee. (*See* Attachment A.) SA Force is the undercover agent whom Ulbricht allegedly hired to arrange the murder-for-hire, as described in that indictment. He is now being investigated by USAO-San Francisco for, among other things, leaking information about USAO-Baltimore's investigation to Ulbricht in exchange for payment, and otherwise corruptly obtaining proceeds from the Silk Road website and converting them to his personal use.

SA Force played no role in the investigation of Silk Road conducted by the U.S. Attorney's Office for the Southern District of New York ("USAO-SDNY," or "this Office"), which proceeded on a separate and independent track from the investigation conducted by USAO-Baltimore. Moreover, the Government does not believe that the ongoing investigation of SA Force is in any way exculpatory as to Ulbricht or otherwise material to his defense. However, in an abundance of caution, the Government seeks to disclose the investigation of SA Force to the defense, and therefore respectfully requests a protective order authorizing the

Government to do so pursuant to Federal Rule of Criminal Procedure 6(e)(3)(E) and prohibiting the defense from disclosing the investigation to any third-party.

Facts

SA Force is being investigated by USAO-San Francisco for a variety of conduct, including suspected misconduct undertaken in his capacity as a DEA undercover agent in USAO-Baltimore's Silk Road investigation. USAO-San Francisco began investigating SA Force in the spring of this year after learning of suspicious transactions he had had with a certain Bitcoin exchange company with a presence in San Francisco. Further investigation by USAO-San Francisco revealed that SA Force held accounts at multiple Bitcoin exchange companies in his own name, through which he had exchanged hundreds of thousands of dollars' worth of Bitcoins for U.S. currency during 2013 and 2014 and transferred the funds into personal financial accounts. USAO-San Francisco also learned that SA Force had used his position as a DEA agent to protect these funds, including sending out an unauthorized administrative subpoena to one of the Bitcoin exchange companies, purporting to instruct the company to unfreeze an account held in SA Force's name that the company had frozen due to suspicious activity.

Since learning this information, USAO-San Francisco has been investigating, among other things, how SA Force could have come into possession of such a large quantity of Bitcoins and the extent to which he may have acquired these Bitcoins through his involvement in USAO-Baltimore's Silk Road investigation. This Office has been assisting USAO-San Francisco with its investigation, by sharing relevant evidence collected from this Office's investigation of Silk Road, including evidence from the server used to host the Silk Road website (the "Silk Road Server") and evidence from Ulbricht's laptop computer. To date, USAO-San Francisco's investigation has uncovered several possibilities as to how SA Force could have acquired a large amount of Bitcoins through his involvement in USAO-Baltimore's Silk Road investigation.

1. Leaks of Investigative Information in Exchange for Payment

As discussed further below, SA Force operated an authorized undercover account on Silk Road under the username "nob," which was involved in the murder-for-hire alleged in the USAO-Baltimore indictment. However, USAO-San Francisco now suspects SA Force of also operating at least two other accounts on Silk Road, which were not authorized undercover accounts. These accounts appear to have been used to leak (or offer to leak) investigative information to Ulbricht (whom SA Force knew only by his Silk Road username, "Dread Pirate Roberts"), in exchange for payment in Bitcoin.

One of these accounts is the Silk Road username "french maid." Evidence from the Silk Road Server and Ulbricht's laptop indicates that, in or about mid-September 2013, a Silk Road user named "french maid" contacted "Dread Pirate Roberts" via Silk Road's private message system, claiming that "mark karpeles" had given the true name of "Dread Pirate Roberts" to "DHLS." Mark Karpeles is the former CEO of a now-defunct Bitcoin exchange company known as "Mt. Gox," whom USAO-Baltimore was seeking to interview in September 2013 to determine if he had any information concerning the identity of the Silk Road operator "Dread Pirate Roberts." "DHLS" is a possible reference to the Department of Homeland Security,

agents of which were working with USAO-Baltimore's investigation. Evidence from Ulbricht's laptop indicates that Ulbricht paid "french maid" $100,000 in Bitcoins to pass on the name that Karpeles had supposedly given to authorities, but that "french maid" never replied.[1] Given "french maid's" use of SA Force's first name and apparent knowledge of the USAO-Baltimore investigation with which he was involved, USAO-San Francisco is investigating whether the "french maid" account was controlled by Force and used to corruptly obtain this $100,000 payment from Ulbricht.

SA Force is also being investigated for leaking investigative information to Ulbricht through a different Silk Road username – "alpacino" (or "albertpacino" or "pacino"). A file recovered from Ulbricht's laptop titled "le_counter_intel" (*i.e.*, "law enforcement counter intelligence") contains extensive records of communications that appear under the heading "correspondence with alpacino." The communications purport to be from someone claiming to be "in the perfect spot to play spy for Silk Road with the DEA." Like the correspondence from "french maid," these communications reflect inside knowledge of USAO-Baltimore's investigation of Silk Road. Further evidence indicates that Ulbricht paid "alpacino" a salary of $500 per week to supply such information. Accordingly, USAO-San Francisco is investigating whether SA Force controlled this username as well and exploited it to exchange investigative information to Ulbricht for payment in Bitcoins.[2]

2. Use of Cooperator's Silk Road Account to Steal Bitcoins from Silk Road

SA Force is also being investigated concerning a theft of $350,000 in Bitcoins that appear to have been taken from Silk Road through the account of a Silk Road employee – the same employee at issue in the murder-for-hire allegations charged by USAO-Baltimore. The employee, Curtis Green, who went by the username "Flush" on Silk Road, was a cooperator in USAO-Baltimore's investigation at the time, and his handler was SA Force. Green was arrested by SA Force and several other agents involved in the USAO-Baltimore investigation on January 17, 2013. Green cooperated with the investigation following his arrest and turned over his login credentials to the "Flush" account to SA Force. According to DEA investigative reports filed by SA Force, SA Force initially changed the password on the "Flush" account; however, the reports state that, on or about January 19, 2013, he gave Green the changed password, so that Green could log in to the account and resume communications with "Dread Pirate Roberts" for the purpose of acting as a confidential source.[3]

[1] Ulbricht's name was not in fact given by Mark Karpeles to any investigators associated with USAO-Baltimore's investigation.

[2] Silk Road employees are known to have been paid in Bitcoin.

[3] All of this information has already been disclosed to the defense, as SA Force's investigative reports were turned over in discovery pursuant to Rule 16(a)(1), given that they contain numerous recorded statements by the defendant.

Approximately one week later, on January 26, 2013, the "Flush" account appears to have been used to steal approximately $350,000 in Bitcoins from Silk Road.[4] "Dread Pirate Roberts" messaged "Flush" on January 26, 2013, accusing him of stealing the money and warning that he was "taking appropriate action." Subsequent private messages from the Silk Road Server and chats recovered from Ulbricht's computer reflect that Ulbricht subsequently recruited a Silk Road user he knew as "nob" to have Green killed in retaliation for the theft. The "nob" account, as noted above, was an undercover account controlled by SA Force. SA Force had been using the account to communicate with "Dread Pirate Roberts," posing as a large-scale drug dealer seeking to do business on Silk Road. As reflected in USAO-Baltimore's indictment, after being solicited to arrange Green's murder, SA Force continued communicating with "Dread Pirate Roberts" about what he wanted done and eventually staged Green's murder to prove that the murder was carried out, for which "Dread Pirate Roberts" paid $80,000.

SA Force's use of the "nob" account for this purpose was part of an authorized law enforcement operation and his communications with "Dread Pirate Roberts" about the murder-for-hire – which have already been disclosed to the defense – are not suspected of being improper. Moreover, the receipt of the $80,000 payment for the murder-for-hire is documented in SA Force's reports. However, the apparent theft of $350,000 from Silk Road through the use of the Green's "Flush" account remains unaccounted for. Given that SA Force had the login credentials to the "Flush" account at the time, he is under investigation for using the account to steal the funds.[5] Although these funds were criminal proceeds and thus would have been subject to seizure by law enforcement, USAO-San Francisco is investigating whether SA Force took the funds without proper authorization and unlawfully converted them to his own personal use.

3. Receipt of Additional Undocumented Payments from "Dread Pirate Roberts"

SA Force continued to use the "nob" account to communicate with "Dread Pirate Roberts" through September 2013, and USAO-San Francisco is investigating whether he used the "nob" account to receive any payments that are not documented in his investigative reports filed with the DEA. In particular, the Silk Road Server contains private messages sent by "Dread Pirate Roberts" to "nob" in the summer of 2013, referencing two transfers of Bitcoins made by "Dread Pirate Roberts" to "nob" during this time period – totaling 400 Bitcoins and 525 Bitcoins, respectively (equivalent to approximately $85,000 altogether at then-prevailing exchange rates). However, the receipt or seizure of these Bitcoins does not appear to be reflected in SA Force's

[4] As a Silk Road administrator, "Flush" had administrative privileges on the Silk Road website that gave him certain effective access to user funds, such as the ability to reset user passwords and thereby take over user accounts.

[5] According to an investigative report filed by SA Force, Green claimed not to know anything about the theft. The report states: "GREEN has telephoned SA Force on numerous occasions and advised that he has been 'racking his brain' about the supposed theft of $350,000 from DREAD PIRATE ROBERTS. Note, DREAD PIRATE ROBERTS is accusing GREEN of stealing the money. GREEN believes that there is a glitch in the website and that somebody hacked into the SILK ROAD marketplace and stole the Bitcoin."

reports. Accordingly, USAO-San Francisco is investigating whether he wrongfully used the "nob" account to acquire these Bitcoins as well and convert them to his personal use.

Discussion

Federal Rule of Criminal Procedure 6(e) generally prohibits an attorney for the Government from disclosing any "matter occurring before the grand jury." Fed. R. Crim. P. 6(e)(2)(B). The Supreme Court has explained that grand jury secrecy is justified, among other reasons, by the need to protect the integrity of an ongoing investigation and to prevent premature public disclosure of the fact that an individual is suspected of criminal wrongdoing. *See Procter & Gamble Co*., 356 U.S. at 681 n. 6. However, the secrecy requirement of Rule 6(e) is not absolute. In particular, the rule provides that a court "may authorize disclosure – at a time, in a manner, and subject to any other conditions that it directs – of a grand jury matter . . . preliminarily to or in connection with a judicial proceeding." Fed. R. Crim. P. 6(e)(3)(E). Disclosure is permissible under this exception if a court presiding over a judicial proceeding determines that "a particularized need for disclosure outweigh[s] the interest in continued grand jury secrecy." *Douglas Oil Co. of Cal. v. Petrol Stops Nw*., 441 U.S. 211, 223 (1979).

Here, the Government seeks to disclose to the defense the facts set forth above concerning the pending grand jury investigation of SA Force, under a protective order that addresses the need to otherwise keep the investigation confidential. The Government therefore requests that the Court enter a protective order authorizing the Government to make this disclosure under Rule 6(e)(3)(E) and precluding the defense from disclosing the existence of USAO-San Francisco's investigation to any third-party.

To be clear, the Government does not believe that this disclosure is required under Rule 16 of the Federal Rules of Criminal Procedure or under *Brady v. Maryland*, 373 U.S. 83 (1963). The suspected criminal conduct for which SA Force is being investigated – even if he did in fact commit the conduct – does not exculpate Ulbricht in any way or otherwise materially aid his defense. To the contrary, the suspected leaks of investigative information by SA Force indicate that Ulbricht repeatedly paid a government agent to provide "counter-intelligence" information in the interest of protecting Silk Road from law enforcement. Likewise, regardless of whether SA Force or someone else stole $350,000 through the "Flush" account in January 2013, the facts remain that Ulbricht believed that his employee, Curtis Green, had stolen the funds, and that Ulbricht sought to murder Green for doing so. Finally, any personal use of payments that SA Force received through his undercover "nob" account reflects only corruption on SA Force's part, rather than anything suggestive of Ulbricht's innocence.

Moreover, SA Force played no role in this Office's investigation of Silk Road and the Government does not intend to call SA Force as a witness at trial. Thus, the facts underlying the USAO-San Francisco investigation do not constitute impeachment material for which disclosure would be required under *Giglio v. United States*, 405 U.S. 150 (1972). Nor does the Government intend to use at trial any communications between Ulbricht and SA Force that were found on the Silk Road Server and Ulbricht's laptop – even though these communications include highly

incriminating exchanges reflecting Ulbricht's hiring of "nob" to arrange the murder of Curtis Green.[6]

Although not exculpatory or impeachment material, in an abundance of caution, the Government seeks to disclose USAO-San Francisco's investigation of SA Force to the defense in order to avoid any dispute concerning whether this information is subject to discovery. Even though the disclosure relates to an ongoing grand jury investigation, the Government believes that, with the entry of a protective order prohibiting further disclosure, the disclosure will be sufficiently limited so as to avoid impinging on any interests protected by Rule 6(e), and that the disclosure is therefore permissible under Rule 6(e)(3)(E). This Office has consulted with USAO-San Francisco, which consents to the proposed disclosure under the requested protective order.

Conclusion

For the reasons set forth above, the Government respectfully requests that the Court enter a protective order authorizing the Government to disclose to the defense the facts set forth in this letter and prohibiting the defense from disclosing the existence of USAO-San Francisco's investigation of SA Force to anyone outside the defense team. The Government further respectfully requests that the protective order, and this letter, be maintained under seal.

Respectfully,

PREET BHARARA
United States Attorney

By: _____
SERRIN TURNER
Assistant United States Attorneys
Southern District of New York

Encl.

[6] The Government does intend to introduce other evidence of this attempted murder-for-hire, through communications that Ulbricht had about it with co-conspirators.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. –

ROSS WILLIAM ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

UNDER SEAL

14 Cr. 68 (KBF)

ORDER

Upon the attached letter from Serrin Turner, Assistant United States Attorney for the Southern District of New York, dated November 21, 2014 (the "Letter"), IT IS HEREBY ORDERED as follows:

1. Pursuant to Rule 6(e)(3)(E) of the Federal Rules of Criminal Procedure, the Government may disclose to the defense the existence of the grand jury investigation referenced in the Letter.

2. Pursuant to Rule 16(d)(1) of the Federal Rules of Criminal Procedure, the defense is prohibited from disclosing the grand jury investigation referenced in the Letter to anyone outside the defense team.

3. The Letter and this Order shall be sealed until such time as the Court otherwise directs.

Dated: New York, New York
November ___, 2014

_____
HON. KATHERINE B. FORREST
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

ROSS WILLIAM ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

UNDER SEAL

14 Cr. 68 (KBF)

ORDER

Upon the attached letter from Serrin Turner, Assistant United States Attorney for the Southern District of New York, dated November 21, 2014 (the "Letter"), IT IS HEREBY ORDERED as follows:

1. Pursuant to Rule 6(e)(3)(E) of the Federal Rules of Criminal Procedure, the Government may disclose to the defense the existence of the grand jury investigation referenced in the Letter.

2. Pursuant to Rule 16(d)(1) of the Federal Rules of Criminal Procedure, the defense is prohibited from disclosing the grand jury investigation referenced in the Letter to anyone outside the defense team.

3. The Letter and this Order shall be sealed until such time as the Court otherwise directs.

Dated: New York, New York
~~November __, 2014~~
December 1, 2014

HON. KATHERINE B. FORREST
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	14 Cr. 68 (KBF)
-v-	SEALED ORDER
ROSS WILLIAM ULBRICHT, Defendant.	

KATHERINE B. FORREST, District Judge:

A conference in this matter is scheduled for Monday, December 15, 2014 at 10:00 a.m. In advance of that conference and not later than 9:00 a.m. that day, the Government shall respond, by letter, to the following:

1. Is the fact of, or any aspect of the Government's investigation of Carl Force public or otherwise known to persons or entities outside of the grand jury, the investigators directly involved in that case or any cases involving Mr. Ulbricht?
2. Does Mr. Force know he is under investigation?
3. If the fact of the investigation is not publicly known, what (if any) harm would the Government suffer if it became known?
4. What's the status of the investigation?

5. Would the Government be able to reveal any of the facts regarding Mr. Force's conduct without endangering the grand jury investigation? If so, which ones? If no facts are known, why not?

SO ORDERED:

Dated: New York, New York
December 12, 2014

KATHERINE B. FORREST
United States District Judge

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

TO BE FILED *EX PARTE* AND UNDER SEAL

December 12, 2014

By Electronic Mail

Hon. Katherine B. Forrest
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross William Ulbricht*, S1 14 Cr. 68 (KBF)

Dear Judge Forrest:

The Government writes *ex parte* to respond to the Court's Order, dated December 12, 2014, which requested additional information regarding the ongoing federal grand jury investigation being conducted by the U.S. Attorney's Office for the Northern District of California ("USAO-San Francisco"), in conjunction with the Public Integrity Section of the Criminal Division of the Department of Justice into Carl Force, a former Special Agent ("SA") with the Drug Enforcement Administration.

After consulting with the Assistant U.S. Attorney in charge of the USAO-San Francisco investigation, we can provide the following responses to your inquiries:

1. The investigation is not public and is only known to a limited group of individuals outside the grand jury and the government employees involved in the investigation case. Specifically, the investigation is known to representatives of Bitstamp (the Bitcoin exchange company that reported the suspicious Bitcoin transactions involving Carl Force that prompted the investigation), outside counsel for Bitstamp, and also, to varying degrees, witnesses who have been interviewed or otherwise contacted as part of the investigation.

2. Carl Force is aware that he is under investigation insofar as he has been interviewed in connection with the grand jury investigation. He is not, however, aware of the full range of misconduct for which he is being investigated.

3. USAO-San Francisco believes that the ongoing grand jury investigation would be harmed by public disclosure of the investigation at this time, for the following reasons:

   a. As noted above, although Carl Force is aware that he is under investigation, he is *not* aware of the full range of misconduct that is the subject of the investigation. Public disclosure of the full scope of the investigation could threaten the integrity of the investigation, as it might cause Mr. Force (or any potential subjects, co-conspirators or aiders and abettors) to flee, destroy evidence, conceal proceeds of misconduct and criminal activity, or intimidate witnesses.

   b. Based on the significant level media attention that the allegations against Carl Force would likely generate, there is a serious risk that media reports could influence the information or testimony provided by witnesses, bias grand jury members, or otherwise impact the integrity of the investigative process.

   c. The grand jury investigation is ongoing and the scope of any charges the Government may end up pursuing against Carl Force is not yet known. Disclosure of the investigation at this juncture would risk publicly airing suspicions or allegations of wrongdoing that may not ultimately be charged due to lack of evidence.

4. According to USAO-San Francisco, the grand jury investigation is at an early stage. The grand jury is scheduled to receive live testimony next Tuesday, December 16, 2014, and is expected to continue into 2015. At this stage it is impossible to pinpoint precisely when charges will be brought, but USAO-San Francisco advises that they anticipate charging Force sometime in mid-2015.

5. At present, for the reasons set forth above in answer #3, the Government does not believe that there any facts that could be released regarding Mr. Force's conduct that may be revealed without jeopardizing the grand jury investigation.

Based on the sensitive nature of the contents of this letter, the Government respectfully requests that the protective order, and this letter, be maintained under seal.

Respectfully,

PREET BHARARA
United States Attorney

By: _____
TIMOTHY T. HOWARD
SERRIN TURNER
Assistant United States Attorneys
Southern District of New York
(212) 637-2308

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

December 17, 2014

TO BE FILED UNDER SEAL

By Email
Hon. Katherine B. Forrest
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross William Ulbricht*, 14 Cr. 68 (KBF)

Dear Judge Forrest:

The Government writes regarding the timing of any additional sealed proceeding the Court intends to hold on the defendant's motion *in limine* concerning the grand jury investigation of former DEA Special Agent Carl Force. The Government respectfully requests that the Court schedule any such proceeding for tomorrow or Friday, rather than holding it today, for two reasons. First, in light of issues raised during the sealed portions of the pretrial conference held on December 15, 2014, the Government respectfully requests leave to file a supplemental letter regarding its position on the matter, and is prepared to file such a letter by 9 a.m. tomorrow, *i.e.*, December 18, 2014. Second, given the expected media presence at the pretrial conference already scheduled for today, the Government respectfully suggests that it would be impractical to hold a sealed portion of that proceeding to discuss the issues surrounding the Force investigation.

Accordingly, to the extent the Court intends to hold an additional sealed proceeding regarding the investigation of Special Agent Force, the Government respectfully requests that the conference be postponed until Thursday or Friday, at the convenience of the Court. The Government also requests that this letter be maintained under seal.

Respectfully,

PREET BHARARA
United States Attorney

By: _____
SERRIN TURNER
TIMOTHY T. HOWARD
Assistant United States Attorneys
Southern District of New York

cc: Joshua Dratel, Esq.

Ordered - under Seal

1. The Court will accept any final submissions on this issue by 9 a.m. tomorrow.

2. To the extent the defendant would request particularized discovery, he should submit a letter setting forth such requests by 9 am tomorrow.

3. The Court shall rule promptly thereafter but does not expect to need an additional hearing on this issue at this time.

KBF
USDJ

12/17/14

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

TO BE FILED UNDER SEAL

December 18, 2014

By Electronic Mail

Hon. Katherine B. Forrest
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross William Ulbricht*, S1 14 Cr. 68 (KBF)

Dear Judge Forrest:

The Government writes regarding the defendant's motion *in limine* to unseal information regarding the ongoing grand jury investigation into a former Special Agent ("SA") with the Drug Enforcement Administration ("DEA"), named Carl Force, and to use that evidence affirmatively at trial. As the Government has previously asserted in prior filings, unsealing the requested information regarding the corruption allegations would result in significant prejudice to the integrity of the ongoing investigation, and the allegations are wholly irrelevant to the Government's case. The information is similarly irrelevant to any potential entrapment defense, previously suggested by defense counsel.[1]

Based on questions posed by the Court during sealed portion of the proceedings, the Government believes that the defendant may be seeking to use allegations from the investigation to support a defense theory that evidence against the defendant has been fabricated. However, as set forth below, the Court should deny the defendant's motion, and preclude the defendant from introducing evidence of alleged corruption by former SA Force at trial because it would have no probative value, and because it would turn the case into a mini-trial of SA Force that would waste time, confuse and mislead the jury, and otherwise unfairly prejudice the Government in violation of Rule 403 of the Federal Rules of Evidence.

[1] The Government addresses these arguments on pages 16 and 17 in its Memorandum of Law in Opposition to the Defendant's Motions in Limine, filed on December 12, 2014.

A. Background

As set forth in the Government's prior submissions, former SA Force was involved in a completely independent investigation into Silk Road based out of the U.S. Attorney's Office for the District of Maryland ("USAO-Baltimore"). The Government's case has not relied on, and is not offering any evidence obtained by, the USAO-Baltimore investigation in this case. The only references to Force that the Government intends to make in its case in chief are to his online undercover identity as "Nob" in TorChat[2] logs recovered from Ulbricht's computer, where the defendant and other co-conspirators mention "Nob" as the party solicited by the defendant to arrange for the murder of Curtis Green, a/k/a "Flush." According to those TorChat logs, the defendant solicited Green's murder because he believed that Green had stolen approximately $350,000 worth of Bitcoins from Silk Road and was concerned that Green may have been cooperating with law enforcement.

The Government long ago produced discovery regarding this incident, including information that the "Nob" account was controlled by an undercover DEA agent, that Curtis Green, a/k/a "Flush" was arrested in January 2013 on narcotics charges and was cooperating with law enforcement, and that the undercover officer had obtained access to the "Flush" account following Green's arrest. The chronology of events regarding Green's arrest and access to the "Flush" account is as follows:

> January 17, 2013
>
> Curtis Green, a/k/a "Flush" was arrested on narcotics charges. "Flush" was a member of the Silk Road support staff and as such could take certain administrative actions with respect to Silk Road user accounts, such as resetting a user's password (*e.g.*, in the event a user claimed to have forgotten his password and needed to create a new one). According to reports filed by Force, Green began cooperating promptly after his arrest and provided Force with access to his "Flush" account; thereafter, Force logged into the "Flush" account and changed the login password in order to secure the account for undercover purposes.
>
> January 19, 2013
>
> According to reports filed by Force, two days later, Force provided Green with the changed password for the "Flush" account, in order to return access to the account to Green, so that Green could cooperate with the investigation by engaging in online conversations with the defendant as a confidential informant.

[2] "TorChat" is an instant-messaging service that enables users to chat over the Tor network. *See* http://en.wikipedia.org/wiki/TorChat. TorChat users can "log" their chats in order to keep a record of them for future reference. The TorChat service was and is unaffiliated with the Silk Road website.

January 26, 2013

One week later, according to a TorChat log recovered from the defendant's computer, on January 26, 2013, at approximately 3:39 a.m., another Silk Road support staff member, with the username "Inigo,"[3] informed the defendant that he had detected a possible theft of approximately $350,000 worth of Bitcoins from Silk Road user accounts, which he believed had been stolen the "Flush" account. Specifically, it appeared to "Inigo" that "Flush" had reset the passwords of individual Silk Road users in order to remove funds from the accounts of those users.

According to reports filed by Force, and as corroborated by TorChat logs recovered from the defendant's computer, on that same day, starting at approximately 10:42 a.m., the defendant engaged in an online TorChat with "Nob" in which he told "Nob" that "Flush's" true identity was Curtis Green, and asked "Nob" if he could arrange to "get someone to force [Green] to return the s funds."

According to another TorChat log recovered from the defendant's computer, approximately six minutes later, at approximately 10:48 a.m., "Inigo" informed the defendant that he had successfully stopped the theft of Bitcoins by resetting "Flush's" password, thereby locking "Flush" out of his account.

Subsequent TorChat logs reveal that the defendant later ordered "Nob" to arrange for Green's execution in exchange for $80,000 in United States currency, and that the defendant later informed both "Inigo" and another associate, with the TorChat username "cimon," that Green had been successfully executed.

* * *

All of the above facts above were provided to the defendant in discovery, and have been at defense's proposal to investigate since that time.[4] The only *new* information, made available to the defendant on December 1, 2013, pursuant to a Court order authorizing disclosure under seal pursuant to Rule 6(e)(3)(E), is that: (1) former SA Force is the subject of an ongoing grand jury investigation being conducted by the United States Attorney's Office for the Northern District of California ("USAO-San Francisco") for using his position as a DEA agent to convert Bitcoins for personal use; and (2) USAO-San Francisco is investigating specifically whether former SA Force could have been responsible for the theft of the $350,000 worth of Bitcoins through the "Flush" account during late January 2013.

[3] "Inigo" has been identified as Andrew Michael Jones, who was indicted for his role as a Silk Road administrator in a separate case pending before Judge Griesa. Jones has pled guilty to the charges.

[4] The Government will provide copies of relevant reports authored by former SA Force to the Court by separate letter, which were previously produced to the defendant in discovery on or about March 21, 2014.

Last evening, undersigned counsel consulted with the lead AUSA in USAO-San Francisco handling the Force investigation, regarding the status of the investigation into whether, specifically, Force converted the $350,000 worth of Bitcoins in late January 2013 through the "Flush" account. The AUSA clarified that the investigation is at a preliminary stage with respect to that incident, and that the investigation has not uncovered any evidence that Force was responsible for any such theft other than motive and opportunity. That is, the investigation into that incident is based only upon evidence that Force improperly converted Bitcoins for personal gain in *other* contexts, and that he had the access to the "Flush" account (possibly along with Curtis Green) at the time that the $350,000 worth of Bitcoins went missing from Silk Road accounts. USAO-San Francisco currently has no evidence to corroborate that Force in fact was responsible for those Bitcoins going missing. In fact, some evidence indicates that Force may have had no involvement and that the Bitcoins may not have been stolen at all. Again, the investigation into this incident is at a preliminary stage.

B. Discussion

For the reasons below, any evidence concerning the potential misconduct by former SA Force being investigated by USAO-San Francisco should not be admitted at trial in this case. Any such evidence would have no probative value under Rule 401, and in particular would lend no support to any defense that evidence has been fabricated against the defendant. Moreover, any probative value such evidence did have would be vastly outweighed by the risk of unfair prejudice to the Government, as it would threaten to turn the trial into a time-consuming corruption inquest into SA Force – who had no involvement in this Office's investigation –with the effect of confusing and biasing the jury and turning their attention away from the charges against the defendant.

Evidence from the USAO-San Francisco investigation is not relevant to any fabrication defense, first and foremost, because USAO-San Francisco has not uncovered any evidence that Force fabricated any evidence against the defendant or the "Dread Pirate Roberts" online persona. Again, the USAO-San Francisco investigation instead concerns only whether Force improperly converted Bitcoins to his personal use. Any theory that Force was involved in fabricating evidence against the defendant would be based on a purely speculative leap from one type of misconduct (corrupt conversion of criminal proceeds for personal gain) to another (fabrication of evidence against the defendant).

In particular, any argument that Force could have used the "Flush" account to take control of the "Dread Pirate Roberts" account to plant incriminating statements by the defendant is not only completely speculative, but is also contrary to the evidence in this case. To take several of many examples:

- Logs of TorChat communications seized from the defendant's laptop computer—which occurred over a completely separate communications system from Silk Road—reflect that the defendant discussed the business of owning and operating Silk Road with his co-conspirators on a daily basis throughout the period that Force had access to the login credentials for the "Flush" account, and long afterwards, without any

reference to losing him access to his Silk Road "Dread Pirate Roberts" administrator account.

- Those same TorChat logs reflect that "Inigo" locked down the "Flush" account on January 26, 2013, shortly after coming to believe that "Flush" was responsible for stealing Bitcoins from the site; hence, the account would have been inaccessible to Force after that time.

- While "Flush" had the capability to reset the passwords of Silk Road user accounts, there is no evidence that he had any ability to reset the password for the "Dread Pirate Roberts" account, nor is there any reason to believe a site administrator would give any such ability to his employees.

- Even assuming the defendant could have ever been locked out of the "Dread Pirate Roberts" account, he still would have controlled the server and computer code underlying the website, and could simply have regained control of the account through that root-level access. (By analogy, if a CEO's email account is hacked, that doesn't mean he thereby loses control of his company. In particular, given that he has ultimate, physical control over the email server on which the account his hosted, he can take whatever steps are necessary to regain control over the account.)

- "Dread Pirate Roberts" at times digitally signed or encrypted his communications using what is known as a "private key" – including after January 2013. In order to send those communications, Force would have had to have that private key; yet it was stored on the defendant's computer. There is no way Force could have obtained it simply by gaining access the "Dread Pirate Roberts" account on Silk Road.

Accordingly, there is no basis to admit evidence of corruption on the part of Force to support any theory that Force fabricated evidence against the defendant. Any conceivable wisp of probative value such evidence would have would be clearly outweighed by the danger of unfair prejudice to the Government. The Government does not intend to call former SA Force as a witness or offer any evidence collected by him. Were the defense nonetheless to introduce inflammatory allegations of corruption on the part of this non-witness former agent, and to launch a fishing expedition into whether he somehow fabricated the evidence being used at trial, the result will surely be to "confuse the issues, sidetrack the trial and impede the jury from deciding the guilt or lack of guilt of the defendant[] based on the evidence in the case," in violation of Rule 403. *United States v. Milan-Colon*, 836 F. Supp. 1007, 1012-14 (S.D.N.Y. 1993) (precluding evidence under Rule 403 of an investigation into officers for stealing money from defendant's car at the time of the arrest, where: (1) the Government did not intend to introduce at trial evidence seized by the officers implicated by the corruption investigation and did not intend to call them as witnesses; (2) many of the corruption allegations remained unsubstantiated; and (3) no evidence from the corruption investigation indicated that evidence was fabricated against the defendants).

CONCLUSION

For the reasons set forth above, as well as the Government's prior submissions, the Government respectfully requests that the Court deny the defendants motion *in limine* to unseal information regarding the ongoing USAO-San Francisco investigation into former SA Force, and preclude the defense from using any information regarding the investigation as evidence at trial, based on Rules 401 and 403 of the Federal Rules of Evidence.

Based on the sensitive nature of the contents of this letter, including references to an ongoing grand jury investigation, the Government respectfully requests that it remain under seal.

Respectfully,

PREET BHARARA
United States Attorney

By:_____
TIMOTHY T. HOWARD
SERRIN TURNER
Assistant United States Attorneys
Southern District of New York

cc: Joshua Dratel, Esq.

JOSHUA L. DRATEL, P.C.
A PROFESSIONAL CORPORATION

29 BROADWAY
Suite 1412
NEW YORK, NEW YORK 10006

TELEPHONE (212) 732-0707
FACSIMILE (212) 571-3792
E-MAIL: JDratel@JoshuaDratel.com

JOSHUA L. DRATEL

LINDSAY A. LEWIS
WHITNEY G. SCHLIMBACH

STEVEN WRIGHT
Office Manager

December 18, 2014

BY ELECTRONIC MAIL

FILED UNDER SEAL

The Honorable Katherine B. Forrest
United States District Judge
Southern District of New York
United States Courthouse
500 Pearl
New York, New York 10007

Re: *United States v. Ross Ulbricht*,
14 Cr. 68 (KBF)

Dear Judge Forrest:

This letter is submitted on behalf of defendant Ross Ulbricht and, in response to the Court's December 17, 2014, endorsement of the government's December 17, 2014, letter, sets forth particularized discovery requests regarding former Drug Enforcement Administration Special Agent Carl Force. This letter is submitted under seal, with a copy to the government, because it relates to a matter still under seal.

Accordingly, Mr. Ulbricht makes the following particularized discovery demands with respect to former SA Force:

(1) bank account records from any and all bank accounts maintained by former SA Force or his spouse in the U.S. or overseas;

(2) records from any and all Bitcoin accounts and/or wallets maintained by former SA Force or any of his aliases;

(3) records of any and all Bitcoin transactions conducted by former SA Force through any Bitcoin accounts and/or wallets;

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.

(4) records of any and all Bitcoin blockchain analyses conducted by the government with respect to former SA Force's Bitcoin accounts, wallets, and/or transactions;

(5) any spending, net worth, or other financial analysis conducted with respect to former SA Force;

(6) the names, addresses, and contact information for any person possessing exculpatory information or material regarding former SA Force in connection with this case;

(7) any and all forensic computer or other electronic analysis or tests conducted with respect to former SA Force in connection with the grand jury investigation of him;

(8) any and all phone records relating to former SA Force and/or the government's investigation of him;

(9) any and all aliases used by former SA Force on the Internet, or otherwise;

(10) the contents of any email accounts operated by former SA Force or any of his aliases;

(11) any and all chats involving former SA Force or any of his aliases on Silk Road, or otherwise;

(12) any forum posts authored by former SA Force or any of his aliases on Silk Road, or otherwise;

(13) any and all blog posts authored by former SA Force or any of his aliases;

(14) the contents of any and all social media accounts operated by former SA Force or any of his aliases (including but not limited Facebook, Linkedin, and/or Twitter);

(15) former SA Force's tax returns from 2010 through 2014;

(16) any and all stock or other financial holdings maintained by former SA Force or any of his aliases;

(17) any and all reports prepared by the government regarding its investigation of former SA Force;

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.

(18) any and all reports or other memorialization and/or recording of the interview of former SA Force by government investigators in connection with the current grand jury investigation of him;

(19) any and all search and/or eavesdropping warrant applications and supporting materials, and search and/or eavesdropping warrants executed during the investigation of former SA Force, and the fruits of those searches;

(20) any and all subpoena returns obtained during the government's investigation of former SA Force;

(21) any and all other documents and information obtained by any other process, including but not limited to, pen registers, trap and trace orders, and/or orders pursuant to 18 U.S.C. §2703(d);

(22) any negative or adverse disciplinary records or reports regarding former SA Force;

(23) any FBI rap sheet or other criminal history information regarding former SA Force;

(24) any surveillance footage taken during the government's investigation of former SA Force;

(25) any and all audio recordings of former SA Force made in connection with the investigation of him or of this case;

(26) any other exculpatory information or material regarding former SA Force in connection with this case;

(27) any and all reports, memoranda, recordings, and/or other memorialization of interviews with Curtis Green (a/k/a "Flush") in connection with this case and/or the investigation of former SA Force;

(28) records of any other investigations of former SA Force by the FBI, or any other agency.

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.

Accordingly, it is respectfully requested that the Court compel the government to produce the above-demanded discovery.

Respectfully submitted,

Lindsay A. Lewis

LAL/

cc: Serrin Turner
Timothy T. Howard
Assistant United States Attorneys

Ordered [under seal]

1. The Government shall respond to this letter as soon as practicable. The Government shall consider what information as to which it ~~objects~~ believes subpoenas from the defendant might issue without harming any ongoing investigations.

2. The defendant shall provide the Court and Government forthwith with some prioritization/ranking of the requested items -- otherwise, it's not "particularized" in any helpful sense.

12/18/14

K B. F
USDJ

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
-v-	:	14-cr-68 (KBF)
ROSS WILLIAM ULBRICHT,	:	SEALED MEMORANDUM & DECISION[1]
Defendant.	:	

KATHERINE B. FORREST, District Judge:

On November 21, 2014, the Government submitted a letter (the "November 21, 2014 Letter" or the "Letter") disclosing an ongoing federal grand jury investigation of a former special agent of the Drug Enforcement Agency ("DEA"), Carl Force ("SA Force" or "Force"), by the U.S. Attorney's Office for the Northern District of California ("USAO-San Francisco"), in conjunction with the Public Integrity Section of the Criminal Division of the Department of Justice. In sum and substance, the grand jury investigation (the "Force Investigation") concerns an inquiry into whether Force "went rogue" at some point during an independent investigation of Silk Road by the U.S. Attorney's Office for the District of Maryland ("USAO-Baltimore")—stealing bitcoins, corruptly converting proceeds from Silk Road transactions to his own use, and/or providing inside information regarding the USAO-Baltimore investigation to an individual known as "Dread Pirate Roberts" ("DPR"). DPR is alleged to have controlled the Silk Road website. The Force Investigation is active and its scope is non-public. Notably, the November 21 Letter

[1] References to defendant's ex parte submissions have been redacted from this version of the Sealed Memorandum & Decision.

does not disclose known facts regarding Force's conduct, but rather discloses the fact and scope of an investigation into potential misconduct.

The Government requested leave to disclose the November 21, 2014 Letter to defense counsel pursuant to Rule 6(e)(3)(E) of the Federal Rules of Criminal Procedure under a protective order prohibiting outside disclosure of the Letter and its contents. At that time, the Government asserted—and it continues to assert—that the disclosure is not pursuant to any Brady obligation as the information contained in the Letter is neither exculpatory nor material to any potential defense. On December 1, 2014, the Court granted the Government's request to provide the Letter to defendant pursuant to a protective order.

The parties filed motions in limine on December 9, 2014. As one of his motions, defendant moved for an order unsealing the November 21, 2014 Letter.[2] The Government opposed.[3] On December 15, 2014, the Court held a sealed hearing on the motion. The parties subsequently submitted additional correspondence on this issue, including a second ex parte letter by the defense.

During the December 15, 2014 hearing, the Government argued that significant information regarding what is actually known about Force's role in the investigation of Silk Road by USAO-Baltimore had long ago been disclosed to the defense in discovery. Documents subsequently produced by the Government

---

[2] Defendant's motion in limine was accompanied by an ex parte letter-motion to unseal.

[3] On December 12, 2014, the Government submitted an ex parte letter providing responses to the Court's inquiries regarding the ongoing grand jury investigation of SA Force. A redacted version of this ex parte letter has been provided to the defendant.

confirmed this.[4] The defense maintained that the issues under investigation by USAO-San Francisco might have a significant bearing on this case, and that while certain information was received as part of ordinary pre-trial disclosures, information regarding Force's potentially rogue conduct was not. Based on the discussion at the hearing and all of the submissions on this issue to date, it is clear that precisely what Force did (or did not do) remains unknown.

On December 18, 2014, defendant submitted a lengthy list of extremely broad discovery requests—seeking 28 separate categories of information relating to SA Force from the Government. Defendant has not sought to obtain truly targeted discovery from the Government or any third party. The Government has opposed disclosure of any of the discovery requested on the basis that it would interfere with the ongoing grand jury investigation.

Currently before this Court are the two related motions by defendant: to unseal the November 21 Letter and to compel the Government to produce the 28 enumerated categories of discovery. Notably, none of defendant's submissions explains why it is necessary to have the entirety of the November 21 Letter unsealed and made part of the public record—versus requesting public disclosure of particular isolated facts from that Letter. Nor has the defendant attempted to demonstrate how and why his discovery requests are appropriate under the rules and in light of the Government's assertions regarding the potential impact on the

[4] The Government produced a binder of documents relating to Force's role in the investigation—all of which had been previously disclosed to defendant. These documents reveal the type of technical access Force had to the Silk Road website as part of his work for the DEA on the USAO-Baltimore investigation.

ongoing investigation. Nevertheless, the Court has carefully reviewed defendant's arguments and sets forth its ruling below. Both of defendant's applications are DENIED.

I. BACKGROUND[5]

A. SA Force's Role in the USAO-Baltimore Investigation

In 2012 and 2013, SA Force participated in an independent investigation of Silk Road conducted by USAO-Baltimore. USAO-Baltimore has a pending indictment against Ulbricht charging him with, inter alia, soliciting the murder-for-hire of Curtis Green ("Green"), a former Silk Road employee known by the username "Flush." (See November 21, 2014 Letter at 1, 3.) As part of his duties in connection the USAO-Baltimore investigation, SA Force infiltrated the Silk Road website under the username "Nob." (Id. at 2, 4.) Force managed to strike up an online relationship with DPR, who, the Government contends, is the creator and lead administrator of the Silk Road website. At the heart of its case against Ulbricht is the Government's contention that he is DPR.

Acting in his capacity as a special agent for the DEA, SA Force—via his Silk Road identity, Nob—portrayed himself as someone who wished to distribute large quantities of narcotics through Silk Road. (Id. at 4.) In short, Nob was a fictional "big-time drug dealer." In January 2013, DPR solicited Nob to arrange for the murder-for-hire of Green, the owner of the Flush account. (Id.) The Government intends to introduce evidence that DPR believed that Green had stolen

[5] The Court assumes familiarity with the underlying facts of this case.

approximately $350,000 worth of bitcoins, the currency used to effect Silk Road transactions.

According to the Government, the events leading up to the solicitation of the murder-for-hire of Green are as follows.[6] Green was arrested on narcotics charges on January 17, 2013, and began cooperating with the authorities promptly after his arrest. (See id. at 3; Government's Six-Page Letter of December 18, 2014 ("Gov't December 18, 2014 Letter") at 2.) As part of his cooperation, Green provided Force with access to the Flush account. (Gov't December 18, 2014 Letter at 2.) Force changed the login password on the Flush account to secure it for undercover purposes. (Id.)

On January 19, 2013, Force provided Green with the changed password to the Flush account so that Green could engage in online conversations with DPR as a confidential informant. (Id.) On January 26, 2013, a Silk Road support staff member with the username "Inigo"[7] informed DPR that Flush might have reset the passwords of Silk Road users in order to steal approximately $350,000 worth of bitcoins.[8] (Id. at 3.) DPR messaged Flush, accusing him of stealing the money and warning that he was "taking appropriate action." (November 21, 2014 Letter at 4.) Later that day, DPR engaged in an online TorChat with Nob, in which he told Nob

[6] Information regarding these events was provided to the defense in discovery.

[7] Inigo has been identified as Andrew Michael Jones, who was indicted in a separate case pending before Judge Griesa. Jones has pled guilty to the charges.

[8] The November 21, 2014 Letter notes that "[a]s a Silk Road administrator, 'Flush' had administrative privileges on the Silk Road website that gave him certain effective access to user funds, such as the ability to reset user passwords and thereby take over user accounts." (November 21, 2014 Letter at 4 n.4.)

that Flush was Green and asked Nob if he could arrange to "get someone to force [Green] to return the s [sic] funds." (Gov't December 18, 2014 Letter at 3.) A few minutes later, Inigo informed DPR that he had successfully stopped the theft of bitcoins by resetting the password on the Flush account. (Id.) The Government alleges that defendant subsequently ordered Nob to arrange for Green's murder in exchange for $80,000, and that defendant later informed Inigo and another associate—with the TorChat username "cimon"—that Green had been successfully executed. (Id.)

B. The Force Investigation

USAO-San Francisco began investigating Force in the spring of 2014 after learning of suspicious transactions that Force had with a certain Bitcoin exchange company. (November 21, 2014 Letter at 2.) Further investigation revealed that Force held accounts at several Bitcoin exchange companies, exchanged hundreds of thousands of dollars' worth of bitcoins for U.S. currency during 2013 and 2014, and transferred the U.S. currency into personal accounts. (Id.) USAO-San Francisco also learned that Force used his position as a DEA agent to protect these funds. (Id.) After learning this information, USAO-San Francisco has been investigating, inter alia, how SA Force acquired such a large quantity of bitcoins and whether he did so through exploiting his role in the USAO-Baltimore investigation. (Id.)

In particular, USAO-San Francisco is investigating whether SA Force may have (1) leaked information about the USAO-Baltimore investigation to Ulbricht in exchange for payment, (2) himself used access to Green's Flush account to steal the

$350,000 in bitcoins, and/or (3) received and converted to personal use payments from DPR of approximately $85,000 in bitcoins. (See id. at 2-5; Memorandum of Law in Opposition to the Defendant's Motions In Limine ("Gov't Opp.") at 15.)

The Government has represented that (1) Force did not play any role in the investigation that culminated in Ulbricht's indictment in this District, (2) the Government will not call Force as a witness at trial, and (3) the Government will not use any evidence obtained in the USAO-Baltimore investigation in this case. (Gov't Opp. at 16.) The Government also has represented that it will not seek to introduce at trial any communications between Ulbricht and Force, including communications regarding Ulbricht's alleged hiring of Nob to arrange Green's murder-for-hire. (Id. at 16 n.2.) According to the Government, Nob will be referenced at trial only in connection with TorChat logs in which Ulbricht and his alleged co-conspirators mention Nob as the party that Ulbricht solicited to arrange the murder-for-hire of Green. (See id.; Gov't December 18, 2014 Letter at 2.)

C. Defendant's Asserted Relevance of the Force Investigation

Defendant has submitted two ex parte letters to the Court describing the ways in which information relating to or derived from the Force Investigation might be relevant, material, and exculpatory. According to defendant, [redacted]

[redacted]

D. Defendant's Discovery Requests

On December 18, 2014, defendant submitted a letter under seal that set forth 28 discovery demands for the Government. Together, the demands seek, inter alia, any documents in the Government's possession relating to its investigation of SA Force, including financial analyses, forensic computer analyses, interview notes, reports, warrant applications, evidence obtained via searches and wiretaps, and surveillance footage. The demands also seek any records in the Government's possession regarding SA Force's finances (specifically, records pertaining to his bank, bitcoin, and investment accounts), Internet and telephone communications, and disciplinary records or reports.[9]

II. LEGAL STANDARDS

A. Grand Jury Secrecy

The Supreme Court consistently has "recognized that the proper functioning of our grand jury system depends upon the secrecy of grand jury proceedings." Douglas Oil Co. of Cal. v. Petrol Stops Nw., 441 U.S. 211, 218 (1979) (citation omitted). The fivefold rationale for this policy is

[9] The breadth of the requests is evident on their face. For example, defendant seeks without any other qualification or limitation: "bank account records from any and all bank accounts maintained by former SA Force or his spouse in the U.S. or overseas"; "the contents of any email accounts operated by former SA Force or any of his aliases"; "the contents of any and all social media accounts operated by former SA Force or any of his aliases (including but not limited Facebook, Linkedin, and/or Twitter)"; and "any and all reports prepared by the government regarding its investigation of former SA Force." (Defendant's December 18, 2014 Discovery Requests ("Disc. Requests") ¶¶ 1, 10, 14, 17.)

> (1) To prevent the escape of those whose indictment may be contemplated; (2) to insure the utmost freedom to the grand jury in its deliberations, and to prevent persons subject to indictment or their friends from importuning the grand jurors; (3) to prevent subornation of perjury or tampering with the witnesses who may testify before the grand jury and later appear at the trial of those indicted by it; (4) to encourage free and untrammeled disclosures by persons who have information with respect to the commission of crimes; (5) to protect the innocent accused who is exonerated from disclosure of the fact that he has been under investigation, and from the expense of standing trial where there was no probability of guilt.

In re Grand Jury Subpoena, 103 F.3d 234, 237 (2d Cir. 1996) (quoting United States v. Moten, 582 F.2d 654, 662 (2d Cir. 1978)).

Rule 6(e) implements this policy of secrecy by providing that "[r]ecords, orders, and subpoenas relating to grand-jury proceedings must be kept under seal to the extent and as long as necessary to prevent the unauthorized disclosure of a matter occurring before a grand jury." Fed. R. Crim. P. 6(e)(6). "The plain language of the Rule shows that Congress intended for its confidentiality provisions to cover matters beyond those actually occurring before the grand jury: Rule 6(e)(6) provides that all records, orders, and subpoenas relating to grand jury proceedings be sealed, not only actual grand jury materials." In re Grand Jury Subpoena, 103 F.3d at 237 (emphasis in original).

"[W]hen the district court finds that disclosure of the confidential information might disclose matters occurring before the grand jury, the information should be protected by Rule 6(e)," which means "it receives a presumption of secrecy and closure." Id. at 239 (citation omitted). While this presumption is rebuttable, "[t]he

burden is on the party seeking disclosure to show a 'particularized need' that outweighs the need for secrecy." Id. (quoting Moten, 582 F.2d at 662) (internal quotation marks omitted). "A party makes a showing of particularized need by proving 'that the material they seek is needed to avoid a possible injustice in another judicial proceeding, that the need for disclosure is greater than the need for continued secrecy, and that their request is structured to cover only material so needed.'" Id. (quoting Douglas Oil, 441 U.S. at 222). "If a showing of particularized need has been made, disclosure should occur unless the grand jury investigation remains sufficiently active that disclosure of materials would prejudice a legitimate interest of the government." Moten, 582 F.2d at 663 (citation omitted).

B. Discovery in Criminal Cases

1. Rule 16

"[I]n all federal criminal cases, it is Rule 16 that principally governs pre-trial discovery." United States v. Smith, 985 F. Supp. 2d 506, 521 (S.D.N.Y. 2013). Under Rule 16(a)(1)(E), a defendant is entitled to obtain from the Government documents and objects that are "within the government's possession, custody, or control" if they are "material to preparing the defense."[10] Fed. R. Crim. P. 16(a)(1)(E).

---

[10] Rule 16(a)(1)(E) also permits the defendant to obtain government documents and objects "within the government's possession, custody, or control" if "the government intends to use [them] in its case-in-chief a trial," or if they were "obtained from or belong[] to the defendant." Fed. R. Crim. P. 16(a)(1)(E). Neither scenario applies here. Additionally, under Rule 16(a)(2), the pre-trial discovery authorized by Rule 16 does not encompass "the discovery or inspection of reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case." Fed. R. Crim. P. 16(a)(2). However, Rule 16(a)(2) does not enable the Government to escape potential Rule 16 discovery obligations in this case because the discovery defendant seeks does not concern the investigation or prosecution of

Evidence is "material" under Rule 16 "as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." United States v. Stein, 488 F. Supp. 2d 350, 356-57 (S.D.N.Y. 2007) (quoting United States v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993)). "Evidence that the government does not intend to use in its case in chief is material if it could be used to counter the government's case or to bolster a defense." Id. at 357 (quoting United States v. Stevens, 985 F.2d 1175, 1180 (2d Cir. 1993)). "There must be some indication that the pretrial disclosure of the disputed evidence would . . . enable[ ] the defendant significantly to alter the quantum of proof in his favor." Id. (alterations in original) (quoting United States v. Maniktala, 934 F.2d 25, 28 (2d Cir. 1991)).

A speculative laundry-list discovery request is improper under Rule 16. See, e.g., United States v. Persico, 447 F. Supp. 2d 213, 217 (E.D.N.Y. 2006) (rejecting a discovery request for "long list of items" because the request was based on "mere conjecture"); United States v. Larranga Lopez, 05 Cr. 655 (SLT), 2006 WL 1307963, at *7-8 (E.D.N.Y. May 11, 2006) (Rule 16(a)(1)(E) "does not entitle a criminal defendant to a 'broad and blind fishing expedition among [items] possessed by the Government on the chance that something impeaching might turn up.'" (alteration in original) (quoting Jencks v. United States, 353 U.S. 657, 667 (1957))).

---

the instant case, but rather a different investigation conducted by a different U.S. Attorney's Office concerning a different defendant. See United States v. Armstrong, 517 U.S. 456, 463 (1996) (Rule 16(a)(2) prohibits a defendant from "examin[ing] Government work product in connection with his case." (emphasis added)); United States v. Koskerides, 877 F.2d 1129, 1133-34 (2d Cir. 1989) (purpose of Rule 16(a)(2) is to protect prosecutors' interest in protecting communications concerning trial tactics).

Rule 16(d)(1) provides that the Court may "[a]t any time" deny pre-trial discovery "for good cause," which may be shown "by a written statement that the court will inspect ex parte." Fed. R. Crim. P. 16(d)(1). "[C]ourts have repeatedly recognized that materials . . . can be kept from the public if their dissemination might 'adversely affect law enforcement interests.'" Smith, 985 F. Supp. 2d at 531 (quoting United States v. Amodeo, 71 F.3d 1044, 1050 (2d Cir. 1995)) (collecting cases).

For example, in Smith, the Government sought a protective order for materials concerning an ongoing investigation of possible misconduct in connection with the case. Id. at 516. The Government submitted an ex parte letter that "provided specific details of ongoing investigations that [we]re related to the discovery materials" sought. Id. at 531. The Court ruled that the Government established "good cause" for the protective order under Rule 16(d)(1), noting that the possible public disclosure of an ongoing investigation "could alert the targets of the investigation and could lead to efforts by them to frustrate the ongoing investigations." Id. at 531-35.

2. Rule 17

A party seeking to issue a Rule 17 subpoena must demonstrate that the materials sought are (1) relevant, (2) admissible, and (3) specific. United States v. Nixon, 418 U.S. 683, 700 (1974); see also United States v. Cuti, 528 Fed. App'x 84, 86 (2d Cir. 2013) ("Under Nixon, a party moving for a pretrial Rule 17(c) subpoena, must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." (internal quotation marks omitted)). "Rule 17 subpoenas are properly used to obtain

admissible evidence, not as a substitute for discovery." United States v. Barnes, 560 Fed. App'x 36, 39 (2d Cir. 2014) (summary order) (citing United States v. Murray, 297 F.2d 812, 821 (2d Cir. 1962)).

The party seeking the Rule 17(c) subpoena "must be able to 'reasonably specify the information contained or believed to be contained in the documents sought' rather than 'merely hop[e] that something useful will turn up.'" United States v. Louis, No. 04 Cr. 203, 2005 WL 180885, at *5 (S.D.N.Y. Jan. 27, 2005) (alteration in original) (quoting United States v. Sawinski, No. 00 CR 499(RPP), 2000 WL 1702032, at *2 (S.D.N.Y. Nov. 14, 2000)). Courts in this District have repeatedly noted that Rule 17 does not countenance fishing expeditions; subpoenas cannot simply seek broad categories of documents without an articulation of how they will enable defendants to obtain specific admissible evidence that is probative of defendant's guilt. E.g., United States v. Mendinueta-Ibarro, No. 12 Cr. 379 (VM), 2013 WL 3871392, at *2 (S.D.N.Y. July 18, 2013) ("Subpoenas seeking 'any and all' materials, without mention of 'specific admissible evidence,' justify the inference that the defense is engaging in the type of 'fishing expedition' prohibited by Nixon." (citing Louis, 2005 WL 180885, at *5)); United States v. Binday, 908 F. Supp. 2d 485, 492-93 (S.D.N.Y. 2012) (rejecting Rule 17 subpoena seeking "vast array of documents" because it was "a fishing expedition, not a targeted request for evidentiary matters"); Louis, 2005 WL 180885, at *5 (rejecting Rule 17 subpoena requesting "any and all" documents relating to "several categories of subject matter (some of them quite large), rather than specific evidentiary items").

Rule 17(c)(2) provides that "[o]n motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive." Fed. R. Crim. P. 17(c)(2).

3. Brady

Under Brady v. Maryland, 373 U.S. 83 (1963), the Government has a constitutional duty to disclose favorable and material information to the defendant, id. at 87. However, "Brady is not a rule of discovery—it is a remedial rule." United State v. Meregildo, 920 F. Supp. 2d 434, 440 (S.D.N.Y. 2013) (citing United States v. Coppa, 267 F.3d 132, 140 (2d Cir. 2001)). Brady imposes a disclosure obligation on the Government; it does not give defendant a constitutional entitlement to obtain discovery. See Weatherford v. Bursey, 429 U.S. 545, 559 (1977) ("There is no general constitutional right to discovery in a criminal case, and Brady did not create one . . . ."); see also United States v. Bonventre, No. 10CR228–LTS, 2014 WL 3673550, at *22 (S.D.N.Y. July 24, 2014) (court denied discovery request under Brady because Brady is "not a discovery doctrine that could be used to compel the Government to gather information for the defense"); Meregildo, 920 F. Supp. 2d at 439 ("An interpretation of Brady to create a broad, constitutionally required right of discovery would entirely alter the character and balance of our present systems of criminal justice." (quoting United States v. Bagley, 473 U.S. 667, 675 n.7 (1985))).

III. DISCUSSION

A. Motion to Unseal the November 21, 2014 Letter

It is undisputed that the November 21, 2014 Letter "relates to" an ongoing grand jury investigation, Fed. R. Crim. P. 6(e), such that unsealing the Letter

"might disclose matters occurring before the grand jury," In re Grand Jury Subpoena, 103 F.3d at 239. The Government has repeatedly represented that unsealing information regarding the Force Investigation would result in significant prejudice to the integrity of the investigation. Specifically, the attorneys handling the grand jury investigation believe that disclosure "threatens to harm the investigative process, by revealing to Force or others the full scope of the Government's investigation, which is currently unknown to Force." (See Government's December 19, 2014 Letter at 1.) Such a revelation may cause Force—as well as potential co-conspirators, aiders and abettors, and others—to flee, intimidate witnesses, destroy evidence, and conceal proceeds of criminal activity.[11] (Id. at 2.)

The November 21, 2014 Letter thus is entitled to "a presumption of secrecy and closure." Id. (citation omitted). To overcome this presumption, defendant must make a showing of "particularized need" by proving that disclosure of the November 21, 2014 Letter is "needed to avoid a possible injustice," "that the need for disclosure is greater than the need for continued secrecy," and that defendant's "request is structured to cover only material so needed." Id. (quoting Douglas Oil, 441 U.S. at 222). Defendant has not carried this burden here.

---

[11] The Government's letter of December 12, 2014 sets forth additional reasons why disclosure of the November 21, 2014 Letter threatens to jeopardize the ongoing investigation of SA Force. First, there is a serious risk that the significant level of media attention that the allegations against SA Force would likely generate would "influence the information or testimony provided by witnesses, bias grand jury members, or otherwise impact the integrity of the investigative process." In addition, disclosure of the investigation at this time would risk publicly airing suspicions of wrongdoing that may not materialize due to lack of evidence.

1. "Possible Injustice"

a. Defendant's arguments

Defendant argues that "evidence of an investigation of former SA Force is exculpatory, and thus Brady material.'" (Memorandum of Law in Support of Defendant Ross Ulbricht's Motions In Limine at 29.) Defendant describes the supposed exculpatory value of the November 21, 2014 Letter in two ex parte letters to the Court.

[redacted]

[redacted]

[redacted]

b. Analysis

Defendant has not made a showing that either the fact of the Force Investigation or the information learned during that investigation is "needed to avoid a possible injustice." Contrary to defendant's arguments, the statements in the November 21, 2014 Letter are not exculpatory.[13]

[redacted] In discovery, the Government produced information that (1) the Nob account was controlled by an undercover DEA agent, (2) Green a/k/a Flush was arrested in January 2013 on narcotics charges, and (3) the undercover agent had obtained access to the Flush account

[13] If anything, the November 21, 2014 Letter is inculpatory. The Letter indicates that SA Force may have leaked information about USAO-Baltimore's investigation to DPR in exchange for payment. If Ulbricht is DPR, this is evidence of Ulbricht's criminal state of mind and attempts to protect his criminal enterprise by purchasing investigative information.

after Green's arrest. (Gov't December 18, 2014 Letter at 2.) [redacted]

To whatever extent this provides a basis for a defense, it has been known to the defendant for some time. It is not news. The defense also learned in discovery that the Flush account may have had administrative privileges. In fact, the Government produced evidence that, on January 26, 2013, Inigo told DPR that Flush may have stolen $350,000 in bitcoins by resetting the passwords of Silk Road users. (See id. at 3.) [redacted]

The only new information in the November 21, 2014 Letter is that USAO-San Francisco is investigating whether Force may have stolen the $350,000 in bitcoins, converted other bitcoins to personal use, and/or leaked investigative information to DPR. [redacted] Notably, "USAO-San Francisco has not uncovered any evidence that Force fabricated any evidence against the defendant or the 'Dread Pirate Roberts' online persona." (Gov't December 18, 2014 Letter at 4.) To the contrary, there is persuasive evidence that no such fabrication occurred. (See id. at 4-5.)

Nor does the November 21, 2014 Letter help attack the Government's murder-for-hire allegations. The Government alleges that Ulbricht solicited Green's murder-for-hire in part because he believed that Green had stolen the $350,000 in bitcoins. The fact that SA Force may have been responsible for the theft is irrelevant unless defendant knew about it, and there is no evidence that he did. As the Government correctly points out, "[r]egardless of whether SA Force, Green or anyone else stole the Bitcoins, the identity of the culprit is wholly irrelevant to the fact that the defendant believed that they were stolen by his employee, 'Flush'" (Government's Opp. at 17) and that Flush was Green. [redacted]

[redacted]

Importantly, nothing about the Force Investigation prevents defendant from doing that which he could always do: presenting a theory supported by the technical capabilities of Silk Road and the materials produced in discovery. [redacted] To be clear, to the extent the Government now or at any point in the future develops any exculpatory information, such as information suggesting that Force did fabricate evidence against DPR, it would have a Brady obligation to disclose it to the defense. The Government has affirmed that it fully understands its obligations under Brady, that it currently knows of no exculpatory information, and that, if it acquires any exculpatory material, it will readily produce it to the defense. (See, e.g., Government's December 19, 2014 Letter at 4.) The Court has no reason to believe that the Government has not complied with all of its Brady disclosure obligations to date or that it will not comply with those obligations in the future.

The Court finds that defendant has not met his burden of showing that unsealing the November 21, 2014 Letter is "needed to avoid a possible injustice." The Government's ongoing Brady obligations, as well as its representation that it will not call SA Force as a witness at trial, will not use any evidence obtained in the USAO-Baltimore investigation, and will not seek to introduce any communications between Ulbricht and SA Force further mitigate the (virtually non-existent) risk of "possible injustice" from maintaining the November 21, 2014 Letter under seal.

[redacted]

2. Need for Disclosure Versus Need for Continued Secrecy

Defendant also has not demonstrated that any "need for disclosure is greater than the need for continued secrecy." The grand jury investigation of SA Force is ongoing, and the Government has indicated that unsealing the November 21, 2014 Letter would result in significant prejudice to the integrity of the investigation. The Court credits this statement. In particular, after consultation with USAO-San Francisco, the Government has advised the Court that disclosure of the November 21, 2014 Letter threatens to compromise the investigative process by revealing to SA Force the full scope of the investigation against him. Learning about the full range of misconduct that is the subject of the USAO-San Francisco investigation might jeopardize that investigation by causing Force, and others, to flee, destroy evidence, conceal criminal proceeds, and/or intimidate witnesses. (Government's December 19, 2014 Letter at 2.) Under these circumstances, the Court finds that the minimal, if any, value of the November 21, 2014 Letter to Ulbricht's defense is significantly outweighed by the need for continued secrecy.

3. Structure of the Request

Finally, the Court finds that defendant's request to unseal the November 21, 2014 Letter is not "structured to cover only material" needed to avoid a possible injustice. Rather than requesting to unseal specific facts from the Letter and explaining why disclosure of those facts is necessary for a fair trial, defendant seeks to unseal the entire Letter based on broad, vague allegations that it contains exculpatory information.

In sum, the Court finds that defendant has failed to make a showing of "particularized need" sufficient to overcome the presumption of secrecy. Moreover, even if defendant had made such a showing, the Court nonetheless would conclude that the November 21, 2014 Letter should remain under seal while the grand jury investigation of SA Force is ongoing. See Moten, 582 F.2d at 663 ("If a showing of particularized need has been made, disclosure should occur unless the grand jury investigation remains sufficiently active that disclosure of materials would prejudice a legitimate interest of the government." (emphasis added) (citation omitted)); In re Grand Jury Subpoena, 103 F.3d at 240 ("We have grave doubts as to whether Appellants made a showing of particularized need to the district court. Yet, even were we to decide that they had, we would not favor opening the hearing to the press while the grand jury investigation is on-going.").

Over the course of the trial, defense counsel may find that they have a basis to believe that specific information in the November 21, 2014 Letter is useful or necessary for effective cross-examination. If such a situation arises, defense counsel should so inform the Court and make a proffer as to the probative value of the particular information sought to be disclosed.

B. Defendant's Discovery Requests

Defendant is not entitled to the discovery he seeks either under the Federal Rules of Criminal Procedure or under Brady.

1. Rule 16 Discovery

The evidence defendant seeks does not meet the threshold of materiality required by Rule 16(a)(1)(E), as there is at present no strong indication that the

discovery defendant seeks will play an important role in uncovering admissible evidence or will significantly aid in the preparation of defendant's case. As the Government long ago produced discovery regarding SA Force's access to administrative privileges on Silk Road, the only information that should be new to defendant is that SA Force is being investigated for leaking information, and the conversion and/or theft of bitcoins. Defendant has not articulated a coherent and particular reason why the fact of SA Force's investigation, or the fruits of that investigation, could themselves "counter the government's case" or "bolster a defense." Stein, 488 F. Supp. 2d at 357 (quoting Stevens, 985 F.2d at 1180).

Indeed, this much is made clear by defendant's open-ended laundry list of discovery demands, which represent precisely the kind of speculative fishing expedition not permitted by Rule 16. For instance, defendant seeks discovery as to "bank account records from any and all bank accounts maintained by former SA Force or his spouse in the U.S. or overseas," (Disc. Requests ¶ 1), which could encompass SA Force's spouse's bank statements from the time before she married SA Force. Defendant also seeks "the contents of any email accounts operated by former SA Force or any of his aliases," (Disc. Requests ¶ 10), which could encompass all of SA Force's non-work-related emails and emails relating to investigations other than that of Silk Road. Indeed, eighteen of defendant's twenty-eight requests request "any and all" materials in a particular category, and none is time-delimited. Such broad and speculative requests are inappropriate under Rule 16. To the extent that the defendant requests issuance of truly targeted requests, and can

support those requests under the rules, the Court will review those and make an individualized determination.

Finally, the Court notes that it is not unusual for the Government to investigate many aspects of a criminal case and numerous people involved at the same time, nor (sadly) is this the first occasion on which a court has confronted a situation in which the Government's own investigative team has been accused of misconduct in the course of an investigation. See, e.g., Brown v. United States, No. 1:10 CV 752, 2014 WL 4231063, at *1-2 (N.D. Ohio 2014) (DEA agent indicted by a grand jury on charges of creating incriminating evidence, withholding exculpatory evidence, and committing perjury). The fact that multiple investigations of criminal conduct occur simultaneously does not mean that—even if related as to certain facts—one must or even should await the outcome of the other. It is perfectly appropriate for the Government, in the reasonable exercise of its prosecutorial discretion, to pursue charges as and when it deems it appropriate and necessary. Except in unusual circumstances, courts should not attempt to alter the Government's chosen timing.

In any event, even assuming arguendo that the information defendant seeks is material, good cause exists under Rule 16(d)(1) for denying defendant's request. Here, as in Smith, disclosure of the materials sought by defendant could alert Force to the full scope of the ongoing grand jury investigation and lead to efforts by him to frustrate the investigation. Defendant's pre-trial discovery requests are accordingly DENIED under Rule 16.

2. Rule 17 Subpoenas

In its December 19, 2014 letter, the Government opposed the issuance of any Rule 17 subpoenas based on defendant's discovery requests. Rule 17 subpoenas must be limited to information that is specific, relevant, and admissible. As explained above, defendant's requests collectively seek "any and all" materials with regard to several broad categories of information, and defendant has not articulated any specific items of admissible evidence he seeks. Simply put, were defendant to request the materials he seeks via Rule 17 subpoenas, he would be engaged in "a fishing expedition, not a targeted request for evidentiary matters." Binday, 908 F. Supp. 2d at 492. Further, and again as explained above, the issuance of Rule 17 subpoenas in this case could endanger the ongoing grand jury investigation of SA Force. Accordingly, the issuance of subpoenas based on defendant's discovery requests would be "unreasonable or oppressive" under Rule 17(c)(2), and therefore inappropriate.

3. Brady

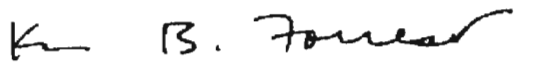
Brady does not provide a vehicle for defendant to obtain the discovery he seeks—it imposes an obligation on the Government to apprise defendant of any exculpatory information obtained via the Force Investigation, but it does not entitle defendant to obtain access to materials from that grand jury investigation, or for that matter any other materials. The Government has an ongoing Brady obligation in this case; this means that to the extent there is any information revealed or developed during the Force Investigation that is material and potentially exculpatory, the Government must disclose such information to the defense.

The Court is aware that defendant argues that the Government cannot know what may be exculpatory as it may not anticipate certain defenses. This is as true here as in any case. To the extent that defendant wants to ensure that the Government provides exculpatory information of which it is aware and that is responsive to a particular theory, it must give the Government enough information to understand that theory. Opening statements are only two weeks away, and the mysteries of the defense theories will be largely revealed at that time; defendant's tactical interest in preserving the mystery of a particular defense theory may now be outweighed by his desire to determine whether particular information supportive of that theory has come to light.

IV. CONCLUSION

For the reasons set forth above, defendant's motion to unseal the November 21, 2014 Letter and discovery requests are DENIED. As explained above, the Court will, over the course of the trial, entertain specific requests to use information from the November 21, 2014 Letter on cross-examination. In addition, if, during the course of the trial, the Government opens the door to specific information or facts develop which render particularized disclosure of facts or documents relevant, the Court will entertain a renewed application at that time.

Dated: New York, New York
December 22, 2014



KATHERINE B. FORREST
United States District Judge

JOSHUA L. DRATEL, P.C.
A PROFESSIONAL CORPORATION
29 BROADWAY
Suite 1412
NEW YORK, NEW YORK 10006

TELEPHONE (212) 732-0707
FACSIMILE (212) 571-3792
E-MAIL: JDratel@JoshuaDratel.com

JOSHUA L. DRATEL
—
LINDSAY A. LEWIS
WHITNEY G. SCHLIMBACH

STEVEN WRIGHT
Office Manager

December 30, 2014

BY ELECTRONIC MAIL

FILED UNDER SEAL

The Honorable Katherine B. Forrest
United States District Judge
Southern District of New York
United States Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross Ulbricht*,
14 Cr. 68 (KBF)

Dear Judge Forrest:

This letter is submitted on behalf of defendant Ross Ulbricht, whom I represent in the above-entitled case, and, in light of the Court's December 22, 2014, Sealed Memorandum & Decision (hereinafter "December 22, 2014 Opinion"), seeks an adjournment of trial until the government completes its grand jury investigation of former Drug Enforcement Administration Special Agent Carl Force, and the full nature of his alleged misconduct is known, and available to Mr. Ulbricht's defense.

The Court's December 22, 2014 Opinion states that "it is clear that precisely what Force did (or did not do) remains unknown." *Id.*, at 3. Yet that is only because it is the government that is in sole possession of that information, and is in exclusive control of the investigation, and because the government's now ten-month long investigation of former SA Force is not complete.

Under such circumstances, Mr. Ulbricht is compelled to request an adjournment of the trial until the government's investigation is complete, and the defense can have access to and the use of the information gathered as a result of the investigation (through either the government or independent means, which at present are foreclosed to the defense).

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.

While the Court's December 22, 2014 Opinion also states, at 22, that the government "has affirmed that . . . if it acquires any exculpatory material, it will readily produce it to the defense[,]"[1] such production during trial or even at this late date would not be sufficient to provide Mr. Ulbricht effective use thereof. Also, obviously, learning of such information *after* trial would be entirely ineffectual.

Similarly, admonishing the government that if it "opens the door" at trial, the issue can be revisited, *id*., at 28, fails to provide Mr. Ulbricht sufficient ability to utilize the information, as investigation and pursuit of documents and other materials cannot be accomplished on such short notice and in the middle of trial. Indeed, the breadth of the defense's discovery requests – all of which are consistent with what the grand jury surely has assembled from various sources – is the result of the lack of the defense's ability to do *anything* at present on its own to pursue the investigation of former SA Force. Delaying that process until mid-trial only amplifies and aggravates the problem therein.

Indeed, in its December 19, 2014, letter to the Court, the government protests that "allowing the defense to pursue the Defense Requests [for discovery] would entail a substantial delay of trial, as both gathering of responsive documents and the opportunity for review by the defense would take several weeks at a minimum." Yet that problem is one of the government's own making given its eleventh-hour disclosure of matters under investigation for the past ten months, and is not a basis for precluding Mr. Ulbricht's use of the information. Rather, it is an indisputable justification for adjourning the trial.

Accommodating the government's desire to maintain the secrecy of its extended investigation of former SA Force and protection of Mr. Ulbricht's constitutional rights are not mutually exclusive interests, and the only solution that accomplishes both objectives is an adjournment of trial. Otherwise, Mr. Ulbricht's Fifth Amendment right to Due Process and a fair trial, and his Fifth and Sixth Amendment rights to prepare and present a defense, will be violated, and he will be denied his Sixth Amendment right to compulsory process, as he would otherwise subpoena former SA Force and/or any other witnesses who could provide testimony at trial.

As noted in my prior December 16, 2014, sealed letter (at n. 2), examining former SA Force without the use of the information disclosed in the government's November 21, 2014, letter – and thereby limited to what suits the government – would be meaningless to the defense.

---

[1] The government's ability even to acknowledge what is "exculpatory" is doubtful given its refusal to acknowledge that what it has already disclosed with respect to former SA Force is exculpatory – even though it is patent that its exculpatory character, rather than any other discovery obligation, is what motivated disclosure "in an abundance of caution."

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.

However, it would be the defense's intention to subpoena former SA Force if the full range of his conduct (and/or misconduct) were accessble for inquiry. Consequently, the defense has prepared a subpoena for former SA Force, and will serve it conditionally, and only on the prosecutors in this case, and not on former SA Force (in order to abide by the Court's ruling denying the motion to unseal the government's November 21, 2014, letter).

In addition, Mr. Ulbricht would be denied his Sixth Amendment right to confrontation, as the government's attempt to introduce former SA Force's undercover identity as "Nob" – through references to him that will involve hearsay, and certainly implicate Nob's communications in significant fashion – in the case without providing Mr. Ulbricht opportunity to cross-examine him (or call him or others as witnesses in any meaningful manner) simply constitutes an attempted end-run around Mr. Ulbricht's Sixth Amendment right to confrontation. Moreover, Mr. Ulbricht's Sixth Amendment right to effective assistance of counsel is also compromised by the limitations placed on counsel's advocacy, investigation, and preparation with respect to former SA Force's alleged misconduct.

The government's effort to use its ongoing grand jury investigation as both a sword and shield cannot be reconciled with Mr. Ulbricht's right to a fair trial. Accordingly, for all the reasons set forth above, as well as in Mr. Ulbricht's previously filed submissions on this subject (as well as the sealed portion of the court conference devoted to this issue), the only appropriate solution is an adjournment of the trial until the government's investigation of former SA Force is complete, and the defense can effectively pursue and ultimately use at trial the information disclosed. Having the trial proceed first puts the cart plainly, and unconstitutionally, before the horse.

Respectfully submitted,

Joshua L. Dratel

JLD/
cc: Serrin Turner
Timothy T. Howard
Assistant United States Attorneys

ORDERED:
The Government shall submit any response not later than 12/31/2014 at 6 P.M.

12/30/2014

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

TO BE FILED UNDER SEAL

December 30, 2014

By Electronic Mail
Hon. Katherine B. Forrest
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross William Ulbricht*, S1 14 Cr. 68 (KBF)

Dear Judge Forrest:

The Government writes respectfully to respond to the defendant's letter submitted under seal earlier today, requesting an adjournment of trial until the conclusion of the pending grand jury investigation of former DEA Special Agent Carl Force. The request essentially seeks to relitigate the issues this Court has already adjudicated in its December 22, 2014 sealed opinion, and should be denied.

The defense's request is premised on the notion that the Force investigation is likely to uncover exculpatory evidence as to the defendant; yet, as the Court has already found, the defense "has not made a showing that either the fact of the Force Investigation or the information learned during that investigation is 'needed to avoid a possible injustice.'" Slip op. at 18. Indeed, the disclosures made by the Government about the investigation to date are "not exculpatory," but rather, "if anything," are "*in*culpatory." *Id.* at 18 & n.13. From the outset, the Government has made clear that the investigation of former SA Force concerns only possible corruption on former SA Force's part rather than anything suggestive of the defendant's innocence. In particular, the investigation does not concern, and has not yielded any indication of, suspected fabrication of evidence, entrapment, or any other conduct by former SA Force that would tend to exculpate the defendant. Accordingly, postponing trial until the Force investigation is over would do nothing except unnecessarily delay these proceedings by several months or longer, to the detriment of the public's right to a speedy trial. *See United States v. Didier* 542 F.2d 1182, 1188 (2d Cir. 1976) ("[T]he right to a speedy trial belongs not only to the defendant, but to society as well.") (internal quotation marks and citation omitted). Again, as stated in the Court's opinion: "The fact that multiple investigations of criminal conduct occur simultaneously does not mean that – even if related as to certain facts – one must or even should await the outcome of the other." Slip op. at 26.

Contrary to the defense's assertion, proceeding with trial will not deny the defendant his "Sixth Amendment right to confrontation." (Ltr. at 3). The Government is not planning to call former SA Force as a witness, and therefore there is no issue of the defendant being deprived of the right to cross-examine him. Nor is the Government is even planning to use any communications of former SA Force as evidence in the case; and even if it were, those communications would not constitute testimonial hearsay implicating the defendant's Sixth Amendment confrontation rights. (Introducing such communications would be no different from introducing a defendant's recorded conversations with an undercover agent on a wiretap or consensual recording, for example.)

As for the defendant's Sixth Amendment right to subpoena witnesses, the Government has never contended that the pending investigation of former SA Force would necessarily prevent the defendant from subpoenaing him to testify *if* the testimony the defendant sought to elicit was material to the defense. However, it appears that the defendant seeks to call former SA Force as a witness merely to elicit the facts surrounding the pending corruption investigation of him. As the Government has previously argued, eliciting such testimony would not merely jeopardize the pending investigation of former SA Force, but it would also plainly be more prejudicial than probative, as it would threaten to turn the trial into a sideshow about former SA Force rather than an adjudication of the guilt or innocence of the defendant. Accordingly, the Government would object to the defense calling former SA Force as a witness simply based on Rules 401 and 403 – regardless of whether the subpoena was issued before or after the conclusion of the grand jury investigation.

In this regard, the Government notes that the defense's letter indicates that the defense has prepared a subpoena for former SA Force to be served "conditionally" on "the prosecutors in this case," as opposed to former SA Force himself. (Ltr. at 3). To the extent the defense means to say that it plans to attempt service of a subpoena on former SA Force by serving the subpoena on the Government, such an attempt at service would be improper. Former SA Force is no longer a federal employee whom the Government has the power to produce at trial; and undersigned counsel are not authorized to accept service on his behalf. Any subpoena served by the defense on former SA Force would thus have to be served personally. However, in order to protect the pending grand jury investigation of former SA Force, the Government respectfully requests that the defense be required to move the Court for permission to serve any trial subpoena on former SA Force, and to give notice to the Government of any such motion, so that the Government has the opportunity to oppose. There is no need for the defense to serve a subpoena on former SA Force merely to trigger litigation over the relevance of his potential testimony. *See United States v. Boyle*, No. 08 Cr. 523 (CM), 2009 WL 484436, at *3 (S.D.N.Y. Feb. 24, 2009) (explaining that requiring a party to make a motion to issue a subpoena is a permissible and advisable procedure where the subpoena is likely to result in a motion to quash).

Accordingly, the Government respectfully requests that the Court deny the defense's request for an adjournment of trial. The Government further respectfully requests that the Court require the defense to move for permission before serving any subpoena on former SA Force, and to notify the Government of such motion, so that the Government may oppose.

Respectfully,

PREET BHARARA
United States Attorney

By: _____
SERRIN TURNER
TIMOTHY T. HOWARD
Assistant United States Attorneys
Southern District of New York

Cc: Joshua Dratel, Esq. (by electronic mail)

Ordered (under seal):
Defendant's motion to adjourn the trial is DENIED. The Court shall provide reasons on the record on January 13, 2015. Any subpoena on former SA Force must be made on motion with notice to the Government. Such a motion would need to be accompanied by a showing that the proposed witness would provide testimony admissible at trial and meet all other applicable rules.
SO ORDERED.

12/31/14

KATHERINE B. FORREST
United States District Judge

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

TO BE FILED UNDER SEAL

February 1, 2015

By Electronic Mail

Hon. Katherine B. Forrest
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross William Ulbricht*, S1 14 Cr. 68 (KBF)

Dear Judge Forrest:

The Government writes to express its objections to proposed Defense Exhibit E (attached to this letter as Exhibit 1), which was provided to the Government on the evening of January 31, 2015. Defense Exhibit E consists of a redacted version of a chat over the Silk Road messaging system between "Dread Pirate Roberts" and "DeathFromAbove," in an apparent attempt to cast Anand Athavale as an alternative perpetrator. As discussed in greater detail below, Defense Exhibit E contains inadmissible hearsay, as it seeks to use statements made by "DeathFromAbove" for the truth in support of an alternative perpetrator theory. Further, it seeks to redact important context from the conversation, which indicates that "DeathFromAbove" was seeking to extort the "Dread Pirate Roberts" based on information regarding the "Dread Pirate Roberts'" attempts to solicit the murder for hire of Curtis Green, a/k/a "Flush." This is a back-door attempt to re-inject former DEA Special Agent Carl Force into the case. When the full version of the conversation is viewed, in the context of evidence recovered from the defendant's laptop and information recently obtained from USAO-San Francisco that Force controlled the "DeathFromAbove" account, it is apparent that there is no probative value to this evidence, and that any potential probative value is substantially outweighed by the potential of unfair prejudice, confusion of the issues, and misleading the jury. Accordingly, to the extent that the defendant makes a spurious claim that this is not being offered for the truth, it should be excluded under Rule 403.

The redactions proposed by the defendant eliminate critical context to the conversation. Defense Exhibit E simply contains references to statements made by "DeathFromAbove" to the "Dread Pirate Roberts," in which "DeathFromAbove" asserts that he believes that "Dread Pirate

Roberts" is Mr. Athavale. The complete version of the conversation as it occurred over the Silk Road messaging system (attached hereto as Exhibit 2) provides important context, indicating that it started on or about April 1, 2013, when "DeathFromAbove" started making accusations that the "Dread Pirate Roberts" was responsible for the disappearance and death of Curtis Green, a/k/a "Flush." The "Dread Pirate Roberts" only responds once during the conversation, in an April 6, 2013 message in which he states:

> I don't know who you are or what your problem is, but let me tell you one thing: I've been busting my ass every god damn day for over two years to make this place what it is. I keep my head down, I don't get involved with the drama and I do the right thing at every turn. Somehow that isn't enough. Somehow psychotic people still turn up at my doorstep. I've been scammed, I've been stolen from, I've been hacked, I've had threats made against the site, I've had threats made against the community, and now, thanks to you, I've had threats made against my life. I know I am doing a good thing running this site. Your threats and all of the other psychos aren't going to deter me. That's all I say to you. I won't answer your questions, or get sucked in to whatever trip you are on. I have much more important things to do. Stop messaging me and go find something else to do.

"DeathFromAbove" continues to make threats of violence against "Dread Pirate Roberts," until, on April 16, 2013 (the portion that the defendant wants admitted) "DeathFromAbove" ultimately provides Mr. Athavale's personal identifiers, and demands a payment of $250,000 in United States currency as "punitive damages" for Green's death, and otherwise threatens to provide information to law enforcement that Mr. Athavale is "Dread Pirate Roberts."

The statements made by "DeathFromAbove" are inadmissible hearsay. They are plainly offered for the truth, in another, utterly frivolous attempt by the defendant to put forward Mr. Athavale as an alternative perpetrator. Any claim by the defendant that this evidence is not offered for the truth is spurious and belied by the defendant's prior improper attempts to seek to have Special Agent Jared DerYeghiayan testify on cross-examination as to his undeveloped *suspicions* of Mr. Athavale at an early stage of his investigation.

Even if not precluded by the hearsay rules, these statements further present a significant danger of unfair prejudice under Rule 403 in supporting an inference of alternative perpetrator, as the record lacks any legitimate evidence that can link Mr. Athavale to the crimes charged. As the Second Circuit has noted, where a defendant seeks to offer evidence that an "alternative perpetrator" committed the crime charged, a court must be especially careful to guard against the danger of unfair prejudice under Rule 403, for "[t]he potential for speculation into theories of third-party culpability to open the door to tangential testimony raises serious concerns." *Wade v. Mantello*, 333 F.3d 51, 61 (2d Cir. 2003). As the Second Circuit explained in *Wade*:

> In the course of weighing probative value and adverse dangers, courts must be sensitive to the special problems presented by

> 'alternative perpetrator' evidence. Although there is no doubt that a defendant has a right to attempt to establish his innocence by showing that someone else did the crime, a defendant still must show that his proffered evidence on the alleged alternative perpetrator is sufficient, on its own or in combination with other evidence in the record, to show a nexus between the crime charged and the asserted 'alternative perpetrator.' It is not sufficient for a defendant merely to offer up unsupported speculation that another person may have done the crime. Such speculative blaming intensifies the grave risk of jury confusion, and it invites the jury to render its findings based on emotion or prejudice.

Id. at 61-62 (quoting *United States v. McVeigh*, 153 F.3d 1166, 1191 (10th Cir.1998) (citation omitted); *see also DiBenedetto v. Hall*, 272 F.3d 1, 8 (1st Cir. 2001) ("Evidence that tends to prove a person other than the defendant committed a crime is relevant, but there must be evidence that there is a connection between the other perpetrators and the crime, not mere speculation on the part of the defendant."); *People of Territory of Guam v. Ignacio*, 10 F.3d 608, 615 (9th Cir. 1993) ("Evidence of third-party culpability is not admissible if it simply affords a possible ground of suspicion against such person; rather, it must be coupled with substantial evidence tending to directly connect that person with the actual commission of the offense."); *Andrews v. Stegall*, 11 Fed. Appx. 394, 396 (6th Cir. 2001) ("Generally, evidence of third party culpability is not admissible unless there is substantial evidence directly connecting that person with the offense.").[1]

Any evidence that Mr. Athavale was an alternative perpetrator must be carefully scrutinized. In order to introduce evidence that Mr. Athavale was the "alternative perpetrator" in this case, the defense must offer evidence of a direct and substantial connection between Mr. Athavale and Silk Road based on *actual fact*. The record simply does not support any such direct and substantial connection. Rather, the only testimony received by the jury regarding Mr. Athavale was testimony from Special Agent DerYeghiayan on cross examination acknowledging that Mr. Athavale: (1) is a Canadian citizen who resided in Vancouver; (2) was at one time connected to "half a page" of different IP addresses; (3) is a libertarian with a profile on the mises.org website; and (4) frequently used terms and spelled words on the mises.org website in a similar manner to the way that "Dread Pirate Roberts" was known to use them on Silk Road, including "labour," "real-time," "lemme," "rout," "intellectual laziness," "agorism," and "agorist." *See Tr.* 672:23-678:25, 813:6-819:9. The association between Mr. Athavale and the charged offenses is insubstantial on this record, such that that Defense Exhibit E "invite[s] testimony that [is] both distracting and inflammatory" and "pose[s] a danger of turning attention away from issues of [defendant's] culpability." *Wade v. Mantello*, 333 F.3d at 61.

The substantial risk of unfair prejudice in the admission of statements by "DeathFromAbove," is further compounded when the full conversation is viewed in the context of other evidence. First, the defendant's computer contained a file, received into evidence as

[1] Additional legal support for these propositions is detailed on page 12 of the Government's prior letter in this matter dated February 1, 2015.

Government Exhibit 241, which reflects the fact that the defendant did not in fact feel threatened by "DeathFromAbove." Specifically, the unredacted version of Government Exhibit 241 (attached hereto as Exhibit 3), reflects the following entries, which correspond in timing and content to the conversation with "DeathFromAbove":[2]

> 04/02/2013
>
> got death threat from someone (DeathFromAbove) claiming to know I was involved with Curtis' disappearance and death. messaged googleyed about it. goog says he doesn't know. user is prolly friend of Curtis who he confided his plan to.
>
> * * *
>
> 4/10/2013
>
> being blackmailed again. someone says they have my ID, but hasn't proven it.
>
> * * *
>
> 4/13/2013
>
> guy blackmailing saying he has my id is bogus

The full context of the conversation makes plain that the defendant received the threat from "DeathFromAbove," and then rejected it as without substance after "DeathFromAbove" repeatedly incorrectly referred to him as "Anand."[3]

Further, it is important to note that it appears that "DeathFromAbove," was controlled by former Special Agent Force, based on information that was recently obtained from USAO-San Francisco regarding their ongoing grand jury investigation into Force. Following the defendant's first attempt to seek to use Defense Exhibit E with Special Agent DerYeghiayan, the Government consulted with the lead Assistant U.S. Attorney handling the Force investigation, who provided evidence that Force controlled the "DeathFromAbove" account and sent the

---

[2] The version of Government Exhibit 241 that was received in evidence is redacted to exclude references to the Curtis Green "murder for hire." The Court previously ruled that the Government was permitted to present evidence regarding the murder-for-hire of Green. Although the Government agreed with the ruling of the Court, it elected to forego presenting evidence regarding that incident at trial, and has redacted references to the incident at the request of defense counsel.

[3] By omitting the full context of the conversation, the defendant also conveniently eliminates the statement by "Dread Pirate Roberts" that he had "been busting my ass every god damn day for over two years to make this place what it is," which is obviously contrary to the defense theory of the case presented during opening argument.

messages to the defendant.[4] Accordingly, when taken in context with the information obtained from the defendant's computer and the fact that "DeathFromAbove" was used by Force, it is evident that the excerpt of the chat is being used to mislead and confuse the jury. Accordingly, because the evidence has no probative value, and any possible probative value is vastly outweighed by the danger of unfair prejudice, confusion of the issues, and misleading the jury, it should be precluded under Rule 403.

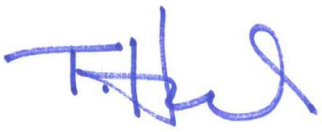
CONCLUSION

For the reasons set forth above, the Government respectfully objects to proposed Defense Exhibit E as inadmissible hearsay. To the extent that the defense makes a spurious application to have it admitted for any purpose other than the truth, Defense Exhibit E should be alternatively excluded under Rule 403 based on the significant danger of unfair prejudice, confusion of the issues, and misleading the jury that the evidence presents.

Based on the sensitive nature of the contents of this letter, including references to an ongoing grand jury investigation, the Government respectfully requests that it remain under seal.

Respectfully,

PREET BHARARA
United States Attorney



By:_____
TIMOTHY T. HOWARD
SERRIN TURNER
Assistant United States Attorneys
Southern District of New York

Cc: Joshua Dratel, Esq.

[4] It should be noted that former Special Agent Force (who was aware of the Curtis Green murder-for-hire attempt) had access to law enforcement reports filed by Special Agent DerYeghiayan concerning his investigation into Mr. Athavale, which is likely the source of the information provided by Force through the "DeathFromAbove" account, in an attempt to extort the defendant.

4/6/13 18:00	DeathFromAbove	Dread Pirate Roberts	Dread Pirate Roberts	It's not that easy Anand [redacted]
4/10/13 11:54	DeathFromAbove	Dread Pirate Roberts	so	[redacted]. Do they have a casino there Anand?
4/16/13 5:56	DeathFromAbove	Dread Pirate Roberts	personal history	Name: Anand Athavale DOB: [redacted] POB: India Citizenship: India Sex: M Brown hair, 5'6" tall, Brown eyes, 300 lbs. Residence: [redacted] is that enough to get your attention? [redacted] So, $250,000 in U.S. cash/bank transfer and I won't give you identity to law enforcement. Consider it punitive damages. DeathFromAbove

Date	To/From	Subject	Message Body
4/1/2013 8:40	From: DeathFromAbove	message for Dread Pirate Roberts	Dread Pirate Roberts, I know that you had something to do with Curtis' disappearance and death. Just wanted to let you know that I'm coming for you. Tuque. You are a dead man. Don't think you can elude me. De Oppresso Liber
4/1/2013 8:43	From: DeathFromAbove	message for Dread Pirate Roberts	Dread Pirate Roberts, I know that you had something to do with Curtis' disappearance and death. Just wanted to let you know that I'm coming for you. Tuque. You are a dead man. Don't think you can elude me. De Oppresso Liber
4/3/2013 7:50	From: DeathFromAbove	I'm coming	Indigo, did you forward the below message to your boss? i'm coming for your ass, also :) "Dread Pirate Roberts, I know that you had something to do with Curtis' disappearance and death. Just wanted to let you know that I'm coming for you. Tuque. You are a dead man. Don't think you can elude me. De Oppresso Liber"
4/5/2013 7:32	From: DeathFromAbove	Dread Pirate Roberts	indigo please pass this message to your boss. FBI, DEA, SOCA, AFP, can't find you but don't think for a second DOD (US Army and Navy) can't. i just want an explanation; if you didn't do it, then I need you to tell me who did. you don't strike me as the Type but I have seen stranger stuff; if I don't hear from you by this weekend then I fly to Vancouver within the next couple of days; DeathFromAbove
4/6/2013 12:37	To: DeathFromAbove	re: Dread Pirate Roberts	I don't know who you are or what your problem is, but let me tell you one thing: I've been busting my ass every god damn day for over two years to make this place what it is. I keep my head down, I don't get involved with the drama and I do the right thing at every turn. Somehow that isn't enough. Somehow psychotic people still turn up at my doorstep. I've been scammed, I've been stolen from, I've been hacked, I've had threats made against the site, I've had threats made against the community, and now, thanks to you, I've had threats made against my life. I know I am doing a good thing running this site. Your threats and all of the other psychos aren't going to deter me. That's all I'll say to you. I won't answer your questions, or get sucked in to whatever trip you are on. I have much more important things to do. Stop messaging me and go find something else to do.
4/6/2013 18:00	From: DeathFromAbove	Dread Pirate Roberts	It's not that easy Anand. I'm legit. Green Beret. Friend of Curtis. I have access to TS/SCI files that FBI, DEA, AFP, SOCA would kill for. In fact, that is what I do ... kill. The only thing that I do. Curtis had a lot of faults but he helped me through a really bad time. I only have one question for you. What did you do with Curtis Green? Tell me the truth and I'll spare you. We, his love ones, need to know. Don't worry DoD has no interest in you and your little website. North Korea and Iran are a lot more important. In fact, as far as the Army and Navy are concerned you are a nobody. Petty drug dealer. But, Curtis was somebody. So tell me where he is and we will can be done with this.
4/10/2013 11:54	From: DeathFromAbove	so	I'm reviewing your file and you don't fit the profile of a killer. So where is Curtis? I need an answer. I got side-tracked from Vancouver, but I think that I'll go to the North Bay Indian Reservation. Do they have a casino there Anand?
4/16/2013 5:56	From: DeathFromAbove	personal history	Name: Anand Athavale DOB: [redacted] POB: India Citizenship: India Sex: M Brown hair, 5'6" tall, Brown eyes, 300 lbs. Residence: [redacted] is that enough to get your attention? After watching you, there is no way you could have killed Curtis. But I think you had something to do with it. So, $250,000 in U.S. cash/bank transfer and I won't give you identity to law enforcement. Consider it punitive damages. DeathFromAbove

03/20/2013
someone posing as me managed to con 38 vendors out of 2 btc each with a fake message about a new silk road posted about cartel formation and not mitigating vendor roundtable leaks.
worked on database error handling in CI

03/21/2013
main server was ddosed and taken offline by host
met with person in tor irc who gave me info on having custom hs guards
buying up servers to turn into hidden service guards

03/22/2013
deployed 2 guards on forum
adjusted check_deposit cron to look further back to catch txns that died with an error

03/23/2013
bought a couple of more servers from new hosts
organized local files
stripped out srsec db naming functions
introduced at least two bugs doing this

03/24/2013
been slowly raising the cost of hedging
orgainzed local files and notes

03/25/2013
server was ddosed, meaning someone knew the real IP. I assumed they obtained it by becoming a guard node. So, I migrated to a new server and set up private guard nodes. There was significant downtime and someone has mentioned that they discovered the IP via a leak from lighttpd.

03/26/2013
private guard nodes are working ok. still buying more servers so I can set up a more modular and redundant server cluster. redid login page.

03/27/2013
set up servers

03/28/2013
being blackmailed with user info. talking with large distributor (hell's angels).

03/29/2013
commissioned hit on blackmailer with angels

04/01/2013
got word that blackmailer was excuted
created file upload script
started to fix problem with bond refunds over 3 months old

04/02/2013
got death threat from someone (DeathFromAbove) claiming to know I was involved with Curtis' disappearance and death. messaged googleyed about it. goog says he doesn't know. user is prolly friend of Curtis who he confided his plan to.
applied fix to bond refund problem
stopped rounding account balance display

04/03/2013
spam scams have been gaining tracktion. limited namespace and locked current accounts.
lots of delayed withdrawals. transactions taking a long time to be accepted into blockchain. Wallet was funded with single large transaction, so each subsequent transaction is requiring change to be verified. lesson: wallets must be funded in small chunks.
got pidgin chat working with inigo and mg

04/04/2013
withdrawals all caught up
made a sign error when fixing the bond refund bug, so several vendors had very negative accounts.
switched to direct connect for bitcoin instead of over ssh portforward
received visual confirmation of blackmailers execution

04/05/2013
a distributor of googleyed is publishing buyer info
mapped out the ordering process on the wiki.
gave angels access to chat server

04/06/2013
made sure backup crons are working
gave angels go ahead to find tony76
cleaned up unused libraries on server
added to forbidden username list to cover I <-> l scam

04/07/2013
moved storage wallet to local machine
refactored mm page

04/08/2013
sent payment to angels for hit on tony76 and his 3 associates
began setting up hecho as standby
very high load (300/16), took site offline and refactored main and category pages to be more efficient

04/09/2013
problem with load was that APC was set to only cache up to 32M of data. Changed to 5G and load is down to around 5/16.
ssbd considering joining my staff
transferring standby data to hecho standby server

04/10/2013
some vendors using the hedge in a falling market to profit off of me by buying from themselves. turned of access log pruning so I can investigate later. market crashed today.
being blackmailed again. someone says they have my ID, but hasn't proven it.

04/11/2013
set up tor relays
asked scout to go through all images on site looking for quickbuy scam remnants
cimon told me of a possible ddos attack through tor and how to mitigate against it.
guy blackmailing saying he has my id is bogus

04/12/2013
removed last remnance of quickbuy scam
implemented new error controller

rewrote userpage

04/13/2013
inigo is in the hospital, so I covered his shift today. Zeroed everything and made changes to the site in about 5 hours

04/14/2013
did support. inigo returned.
started rewritting orders->buyer_cancel, been getting error reports about it.

04/15/2013
day off

04/16/2013
rewrote buyer_cancel

04/17/2013
rewrote settings view

04/18/2013
modified PIN reset system

04/19/2013
added blockchain.info as xrate source and modified update_xrate to use both and check for discrepancies and log.
modified PIN reset system

04/20/2013
migrated to different host because current host would not connect to guards. Bandwidth limited and site very slow after migration.

04/21 - 04/30/2013
market and forums under sever DoS attack. Gave 10k btc ransom but attack continued. Gave smed server access. Switched to nginx on web/db server, added nginx reverse proxy running tor hs. reconfiged everything and eventually was able to absorb attack.

05/01/2013
Symm starts working support today. Scout takes over forum support.

05/02/2013
Attack continues. No word from attacker. Site is open, but occasionally tor crashes and has to be restarted.

05/03/2013
helping smed fight off attacker. site is mostly down. I'm sick.
Leaked IP of webserver to public and had to redeploy/shred
promoted gramgreen to mod, now named libertas

05/04/2013
attacker agreed to stop if I give him the first $100k of revenue and $50k per week thereafter. He stopped, but there appears to be another DoS attack still persisting.

05/05/2013
Attack is fully stopped. regrouping and prioritizing next actions.

05/06/2013
working with smed to put up more defenses against attack

05/07/2013
paid $100k to attacker

05/08/2013
reconfigured nginx to not time out. almost all errors have disappeared.

05/10/2013
started buying servers for intro/guard nodes

05/11/2012
still buying servers

05/13/2013
helping catch up support
smed demo'ed multi address scheme for the forum

05/15/2013
more servers

05/22/2013
paid the attacker $50k

05/26/2013
tried moving forum to multi .onion config, but leaked ip twice. Had to change servers, forum was down for a couple of days.

05/28/2013
finished rewritting silkroad.php controller

05/29/2013
rewrote orders page
paid attacker $50k weekly ransom
$2M was stolen from my mtgox account by DEA
added smed to payroll
rewrote cart page

05/30/2013
spoke to nob about getting a cutout in Dominican Republic. said he knew a general that could help
created misc_cli with send_btc function for sending to many addresses over time.

05/31/2013
$50k xferred to cimon

06/01/2013
someone claiming to be LE trying to infiltrate forum mods

06/02/2013
loaning $500k to r&w to start vending on SR.

06/03/2013
put cimon in charge of LE counter intel

06/04/2013

rewrote reso center

06/05/2013 - 09/11/2013
Haven't been logging. Tried counter intel on DEA's "mr wonderful" but led nowhere. tormail was busted by dea and all messages confiscated. "alpacino" from DEA has been leaking info to me. Helped me help a vendor avoid being busted. did an interview with andy greenberg from forbes where i said i wasn't the original DPR, went over well with community. tried to get a fake passport from nob, but gave fake pic and fucked the whole thing up. nob got spooked and is barely communicating. said his informant isn't communicating with him either. r&w flaked out and disappeared with my 1/2 mil. smed has been working hard to develop a monitoring system for the SR infrastructure, but hasn't produced much in actual results. similarly cimon has been working on the mining and gambling projects, but no results forthcoming. created Anonymous Bitcoin Exchange (ABE) and have been trying to recruit tellers. the vendor "gold" is my best lead at the moment. nod is an H dealer on SR who says he has world class it skills and I am giving him a chance to show his stuff with ABE. did a "ratings and review" overhaul. It hasn't gone over too well with the community, but I am still working on it with them and I think it will get there eventually. tor has been clogged up by a botnet causing accessibility issues.

09/12/2013
Got a tip from oldamsterdam that supertrips has been busted. contacted alpacino to confirm.

09/13/2013
french maid claims that mark karpeles has given my name to DHLS. I offered him $100k for the name.

09/11 - 09/18/2013
could not confirm ST bust. I paid french maid $100k for the name given to DHLS by karpeles. He hasn't replied for 4 days. Got covered in poison oak trying to get a piece of trash out of a tree in a park nearby and have been moping. went on a first date with amelia from okc.

09/19/2013
red pinged me and asked for meeting tomorrow.

09/19 - 09/25/2013
red got in a jam and needed $500k to get out. ultimately he convinced me to give it to him, but I got his ID first and had cimon send harry, his new soldier of fortune, to vancouver to get $800k in cash to cover it. red has been mainly out of communication, but i haven't lost hope. Atlantis shut down. I was messaged by one of their team who said they shut down because of an FBI doc leaked to them detailing vulnerabilities in Tor.

09/30/2013
nod deivered HS tracking service timeline. spoke with inigo for a while about the book club and swapping roles with libertas. Had revelation about the need to eat well, get good sleep, and meditate so I can stay positive and productive.

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.
A PROFESSIONAL CORPORATION

29 BROADWAY
Suite 1412
NEW YORK, NEW YORK 10006

TELEPHONE (212) 732-0707
FACSIMILE (212) 571-3792
E-MAIL: JDratel@JoshuaDratel.com

JOSHUA L. DRATEL
—
LINDSAY A. LEWIS
WHITNEY G. SCHLIMBACH

STEVEN WRIGHT
Office Manager

March 6, 2015

BY ELECTRONIC MAIL

FILED UNDER SEAL

The Honorable Katherine B. Forrest
United States District Judge
Southern District of New York
United States Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States v. Ross Ulbricht*,
14 Cr. 68 (KBF)

Dear Judge Forrest:

This letter is submitted on behalf of defendant Ross Ulbricht, whom I represent, as part of his motion, pursuant to Rule 33, Fed.R.Crim.P., for a new trial. This letter is submitted under seal because it relates to former Drug Enforcement Administration Special Agent Carl Force, and matters previously maintained under seal.

For the reasons set forth below, in addition to those documents and materials listed in Exhibit 1 to Mr. Ulbricht's Rule 33 motion, the government has committed, with respect to former SA Force, two separate nondisclosure violations under the standards of *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny:

(1) former SA Force himself was obligated to disclose any misconduct he committed during the course of or related to his investigation of the Silk Road website, and SA Force's knowledge in that regard is imputed to the prosecution as a whole; and

(2) it is clear from the government's February 1, 2015, letter to the Court (a copy of

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.

> which is attached hereto as Exhibit A) that the grand jury investigation of former SA Force continued to generate exculpatory material and information that the government did not disclose until its letter, and likely has not disclosed at all (with respect to other such information and material).

Regarding former SA Force's knowledge of his misconduct, "a prosecutor's constructive knowledge extends to individuals who are 'an arm of the prosecutor' or part of the 'prosecution team.'" *United States v. Thomas*, 981 F. Supp.2d 229, 239 (S.D.N.Y. 2013), *citing United States v. Gil,* 297 F.3d 93, 106 (2d Cir.2002), and *United States v. Morell,* 524 F.2d 550, 555 (2d Cir.1975); *United States v. Bin Laden,* 397 F.Supp.2d 465, 481 (S.D.N.Y.2005). *See United States v. Millan-Colon*, 829 F.Supp. 620, 634-36 (S.D.N.Y. 1993) (in addition to declaring a mistrial following numerous revelations concerning a corruption investigation into police officers involved in the investigation of the offenses charged, the District Court vacated two guilty pleas entered prior to trial, holding that evidence related to the corruption investigation was material and exculpatory and should have been disclosed as *Brady*/*Giglio* material).

Regarding the continuing generation of undisclosed *Brady* material, the government's February 1, 2105, letter (Exhibit A), at 4, revealed that

> it appears that "DeathFromAbove," was controlled by former Special Agent Force, based on information that was recently obtained from USAO-San Francisco regarding their ongoing grand jury investigation into Force. Following the defendant's first attempt to seek to use Defense Exhibit E with Special Agent DerYeghiayan, the Government consulted with the lead Assistant U.S. Attorney handling the Force investigation, who provided evidence that Force controlled the "DeathFromAbove" account and sent the messages to" Dread Pirate Roberts.

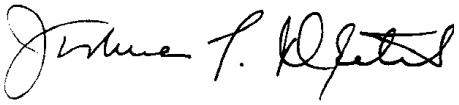
That passage demonstrates that the investigation of former SA Force continued to gather exculpatory information – essentially, that *Brady* material was being collected during the trial itself, and being generated by the investigation of former SA Force. In fact, the government, in its earlier submissions, had never identified the DeathFromAbove username/account as being controlled by former SA Force. Yet during trial it used the cross-examination of Homeland Security Investigations Special Agent Jared Der-Yeghiayan to continue its investigation of former SA Force, and to generate further *Brady* material, but *without disclosing it to the defense until the eve of the defense case itself.*

As established by the case law and principles discussed in the Memo of Law in support of Mr. Ulbricht's Rule 33 motion, that constitutes a *Brady* violation. Accordingly, for the

LAW OFFICES OF
JOSHUA L. DRATEL, P.C.

reasons set forth above and elsewhere in Mr. Ulbricht's motion, it is respectfully submitted that his motion for a new trial should be granted.

Respectfully submitted,



Joshua L. Dratel

JLD/
cc: Serrin Turner
Timothy T. Howard
Assistant United States Attorneys

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------X

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

- against - :

ROSS ULBRICHT, :

Defendant. :
----------X

REPLY 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 AUTHORITIES

CASES

STATUTES

OTHER

STATEMENT OF THE FACTS

A dramatic event has occurred during the intervening period since Mr. Ulbricht's post-trial motions were filed. Less than two months after trial concluded in this case, the government filed criminal charges against former SA's Force and Bridges in the Northern District of California.

The Complaint against former SA's Force and Bridges (hereinafter the "Force Complaint") was unsealed March 30, 2015. A Department of Justice Press Release, March 30, 2015, "Former Federal Agents Charged With Bitcoin Money Laundering and Wire Fraud," available at <http://www.justice.gov/opa/pr/former-federal-agents-charged-bitcoin-money-laundering-and-wire-fraud>, summarized the Force Complaint's allegations against former SA Force as follows:

> Force used fake online personas, and engaged in complex Bitcoin transactions to steal from the government and the targets of the investigation. Specifically, Force allegedly solicited and received digital currency as part of the investigation, but failed to report his receipt of the funds, and instead transferred the currency to his personal account. In one such transaction, Force allegedly sold information about the government's investigation to the target of the investigation.

As the Force Complaint itself notes, "[i]n late January 2013, members of the Baltimore Silk Road Task Force, to include BRIDGES and FORCE, gained access to a Silk Road administrator account as a result of the arrest of a former Silk Road employee." Force Complaint, at 5.

According to the Force Complaint, former SA Force "created certain fictitious personas" *id.*, at 3, and used those phony personas to "seek monetary payment, offering in exchange not to provide the government certain information." *Id.* Former SA Force also created fictional

characters, such as "Kevin," a supposed law enforcement insider who was providing the information to Nob (who was former SA Force, in his authorized undercover role, masquerading as a drug dealer), which Nob in turn was corruptly providing to Dread Pirate Roberts (hereinafter "DPR"). *Id.*, at 14.

Also, former SA Force "stole and converted to his own personal use a sizable amount of bitcoins that DPR sent to Force . . ." *Id.*, at 4. Former SA Bridges also illegally acquired Bitcoin from the Silk Road website, and assisted former SA Force in his illegal endeavors. *Id.*, at 41-49.

In describing former SA Force's assumption of the screen name DeathFromAbove, which he used alternately in an attempt to extort DPR, and/or provide inside law enforcement information to DPR, the Force Complaint concludes that former SA Force was the source of certain information in the LE_counterintel file found on Mr. Ulbricht's laptop because the excerpts in that file "contain information that came from a person or persons inside law enforcement, in part because of their substance and in part because of their use of certain terminology and acronyms that are not widely know by the public." Force Complaint, at 12.

As a result, in assessing former SA Force's activities as DeathFromAbove, the Force Complaint posits that such misconduct "demonstrates that FORCE had a history of: (1) creating fictitious personas that he did not memorialize in his official reports or apprise his superiors at the DEA or the prosecutor of; (2) soliciting payments from DPR; (3) providing law-enforcement sensitive information to outside individuals when the disclosure of such information was not authorized and not memorialized in any official report." *Id.*, at 26.

ARGUMENT

C. *The Government's Investigations of Mark Karpeles and Anand Athavale Were Not Mere "Leads" or "Theories" or "Suspicions" or "Hunches"*

In a further effort to excuse its late production of *Brady* material in the guise of 3500 material on the eve of trial, the government's cites, in its Memo of Law, at 18, cases for the proposition that the "prosecution is not required under *Brady* to disclose every lead, theory, suspicion, or hunch entertained by law enforcement agents during their investigation." Yet those cases are patently inapposite.

1. *The Government's Investigation of Mark Karpeles*

SA Der-Yeghiayan's investigation of Mark Karpeles was not a "lead, theory, suspicion, or hunch[.]" Rather, as SA Der-Yeghiayan's 3500 material demonstrates, he swore *two* separate affidavits in support of search warrants for Mr. Karpeles's e-mail accounts, in two different federal districts, over the course of several months, attesting that there was *probable cause* to believe that Mr. Karpeles was engaged in criminal activity related to operating or managing the Silk Road website.[5]

In a May 29, 2013, e-mail from SA Der-Yeghiayan, he attaches a draft affidavit for a search warrant in the Northern District of Illinois. *See* 3505-13 (attached hereto as part of Exhibit 1). Within that affidavit, SA Der-Yeghiayan declares that

> [b]ased on the above information, I believe there is probable cause that the email address magicaltux@gmail.com and the email address mark@tibanne.com will contain information and evidence related to the distribution can [sic] of controlled substances and conspiracy to distribute a controlled substance as well as additional evidence of KARPELES operating as an unlicensed money service

[5] Of course, as discussed **post**, at 45-48, that also inextricably links the various federal investigations, including the Baltimore investigation, of the Silk Road site, and demonstrates the relevance of former SA's Force and Bridges's misconduct to *this* case.

business."

See 3505-20-21 (attached hereto as part of Exhibit 1). *See also* 3505-24-25 (relating to the investigation of Mr. Karpeles and his Bitcoin exchange company, Mt. Gox).

Nearly three months later, August 15, 2013, SA Der-Yeghiayan performed the same function for the *Southern District of New York*. In an e-mail that day to *AUSA Turner*, SA Der-Yeghiayan noted he was "preparing to swear this out today." *See* 3505-205 (attached hereto as part of Exhibit 2). Attached to that e-mail, which was in response to an e-mail from AUSA Turner earlier that day, with the draft affidavit attached (and which was most likely written by AUSA Turner). *Id.*

In the affidavit, at 3505-206-33 (attached hereto as part of Exhibit 2), SA Der-Jeghiayan swears that "there is probable cause to believe that the SUBJECT ACCOUNTS contain evidence, fruits, and instrumentalities of narcotics trafficking and money laundering, . . ." 3505-209-10 (at ¶ 3). *See also* 3505-226, at ¶ 23 ("I respectfully submit there is probable cause to believe that KARPELES has engaged in the SUBJECT OFFENSES").

The affidavit by SA Der-Yeghiayan, ostensibly written by AUSA Turner, states that it is "based on my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers and civilian witnesses." 3505-210 at ¶ 4 (Exhibit 2). Also, it "does not include all the facts that I have learned during the course of my investigation." *Id.*, at ¶ 4.

Specifically, the affidavit also attests that:

- "I believe that KARPELES has been involved in establishing and operating the Silk Road website." 3505-224, ¶ 22. *See also* 3505-267 (July 11, 2012, e-mail from SA Der-Yeghiayan stating, "[w]e think we found out who's behind the [Silk Road]");
- Mr. Karpeles "has the technical expertise and experience necessary in order to establish and operate a large commercial website such as the Silk Road Underground Website." 3505-225, at ¶ 22(c);
- Silk Road "relies on a highly complex system for processing Bitcoins strongly suggests that it was designed by someone with extensive technical expertise related to Bitcoins – which KARPELES, being the owner and operator of a major Bitcoin exchange and Bitcoin discussion forum, clearly has." *Id.*; and
- ". . . in early 2011, around the same time the Silk Road began operating, KARPELES acquired Mt. Gox. Given his ownership of this Bitcoin exchange business, KARPELES had a strong motive to create a large underground marketplace where Bitcoins would be in high demand. The Silk Road website was uniquely well suited to this purpose, as it generated a huge source of demand for Bitcoins. Indeed, as of April 2013, the total value of Bitcoins in circulation topped 1 billion dollars. Because there few legitimate vendors who accept Bitcoins as payment, it is widely believed that the rise of Bitcoins has been driven

in large part by their use on Silk Road." 3505-224-25, at ¶ 22(b).[6]

As part of the SDNY search warrant application, AUSA Turner himself filed a declaration seeking a Sealing Order, in which he affirmed that sealing was necessary "to avoid premature disclosure of the investigation which could inform potential criminal targets of law enforcement interest[.]" 3505-234 (attached as part of Exhibit 2). Thus, AUSA Turner asked the Magistrate Judge to "order the Provider not to notify any person of the existence of the warrant."[7]

Notwithstanding these facts, the government possesses the temerity to describe the investigation of Mr. Karpeles – and the rationale for not disclosing it as *Brady* material – as a "hunch" or "lead" or "theory" or "suspicion." *Probable cause*, determined by the very same prosecutor who tried this case, is exceedingly more substantial than of those ephemeral concepts.

In addition, the government's claim, in its Memo of Law, at 17, that the investigation shifted to Mr. Ulbricht once he was identified as a suspect is again refuted by the record created

---

[6] In an undated report, SA Der-Yeghiayan also stated, "Agents have discovered strong ties between those controlling the bitcoin markets and those operating the Silk Road." 3505-3122-24. *See also id*., ("HSI O'Hare has also identified multiple financial accounts belonging to the Silk Road operators which contain bitcoins equal in value to millions of U.S. dollars" and "[o]ver the last few months, HSI O'Hare has made several breakthroughs in identifying high priority targets believed to be the backbone of the website"). SA Der-Yeghiayan also wrote another, six-page report regarding his then-ongoing investigation of Mr. Karpeles. *See* 3505-3475-80.

[7] That concern about notice related to Mr. Karpeles and his confederates, and not to Mr. Ulbricht, who was not yet a target or even focus of the government's investigation and is not even mentioned in the warrant application. Of course, as discussed **post**, at 56, Mr. Karpeles had already been alerted to U.S. law enforcement's interest in him by the precipitous seizure – by none other than former SA Bridges (likely in concert with former SA Force) – of Mr. Karpeles's accounts at Dwolla, a money exchange business, worth more than $2 million dollars.

by the government itself. For example, September 30, 2013, the day before Mr. Ulbricht's arrest,

SA Der-Yeghiayan requested, "can we also have a copy of their UC chats (and their Seattle counterparts) with DPR to see if there's any language or connections to [Mr. Karpeles] or the vendors we're working." 3505-3512.

The day after Mr. Ulbricht's arrest, October 2, 2013, SA Der-Yeghiayan wrote an e-mail that "after reviewing some notes from [Mr. Ulbricht's] computer last night/this morning there appears to be some inferences to [Mr. Karpeles's] involvement and associations to [Silk Road]." 3505-3020. Also, SA Der-Yeghiayan wrote in an October 7, 2013, e-mail – nearly a week after Mr. Ulbricht's arrest – to AUSA Turner and Internal Revenue Service Special Agent Gary Alford, in response to SA Alford's e-mail regarding an allegedly hacking of the bitcoin forum soon after Mr. Ulbricht's arrest, "I figured MK [Mr. Karpeles] is purging everything after [Mr. Ulbricht's] arrest . . . I know he was initially involved." 3505-707 (ellipsis in original).

A week later, in an October 15, 2013, e-mail, SA Der-Yeghiayan was still providing materials relating to Mr. Karpeles, as he sent AUSA Turner an Excel spreadsheet of "Karpeles Dwolla Transactions" – which consists of nearly one thousand pages. *See* 3505-895, 901-2916. SA Der-Yeghiayan also authored an investigative report dated October 17, 2013, a little more than two weeks after Mr. Ulbricht's arrest, regarding the return on a search warrant served on Google for two of Mr. Karpeles's e-mail accounts. *See* 3505-3869.

At the same time, the government was also reaching out to Mr. Karpeles for information about Mr. Ulbricht. In an October 12, 2013, e-mail to AUSA Turner and SA Alford, SA Der-Yeghiayan, commenting on the source of information about Mr. Ulbricht's Mt. Gox account,

"just heard that information was passed from MK's [Mark Karpeles's] atty's to Baltimore." 3505-895.

Thus, Mr. Karpeles was a subject of the government's investigation from mid-2012 (*see* 3505-267, cited **ante**, at 23) – nearly 18 months – until even after Mr. Ulbricht's arrest, which ultimately occupied the entirety of the prosecution's attention. In fact, as SA Der-Yeghiayan confirmed at trial, the government has never examined any of Mr. Karpeles's electronic devices, or servers, or any of his other e-mail accounts beyond the two covered by the subpoena served upon Google. T. 681-82.

Consequently, the government's claim that its investigation of Mr. Karpeles was insufficiently substantive to constitute exculpatory material and information it was required to disclose is simply unsustainable.

2. ***The Government's Investigation of Anand Athavale***

The government's investigation of Anand Athavale also constituted an inquiry far more substantial than a "hunch," "lead," "theory," or "suspicion." In a November 12, 2012, e-mail, SA Der-Yeghiayan wrote that "[w]e believe we just make a break through recently and have identified the administrator of the website who is residing in or around Vancouver." 3505-318.

The next day, November 13, 2012, SA Der-Yeghiayan described Mr. Athavale at "the target," 3505-316, and "the Vancouver target." 3505-317. *See also* 3505-738-39 (November 19, 2012, e-mail from SA Der-Yeghiayan stating, "[t]his guy I believe [] is the main admin for the website"). SA Der-Yeghiayan would later write, too, that Mr. Athavale "has the computer skills and knowledge to [be] able to operate the Silk Road in the manner in which it appears DPR does[,]" and "has demonstrated the ability to be able to play the part of multiple identities

online." 3505-3084.

In that November 13, 2012, e-mail, SA Der-Yeghiayan also reported that "[w]e also have pages of chats conducted with a UC agent. I took all the chats and message created by the user and was searching key words used by the administrator in another online forum I believe the Admin posts in." 3505-316. Elaborating, SA Der-Yeghiayan explained that he had "spent quite a bit of time analyzing his writing and posts he has made. Even went as far as having an English professor from a major University critique each writing sample[] and who said they could very well be the same person." 3505-317.

SA Der-Yeghiayan prepared a ten-page report regarding his investigation of Mr. Athavale, focusing on Mr. Athavale's background, his extensive internet presence, and a comparison of Mr. Athavale's writing style with that of Dread Pirate Roberts. 3505-591-600 (a copy of which is attached as Exhibit 3). That analysis included 32 separate similarities cited by SA Der-Yeghiayan. 3505-596-97.

SA Der-Yeghiayan's report regarding Mr. Athavale also noted that "HSI O'Hare has identified ATHAVALE as the likely identity behind the SR [Silk Road] administrator username Dread Pirate Roberts by using the posts on the SR Forum, and using the chat sessions recorded by HSI Baltimore." 3505-598. SA Der-Yeghiayan's report explained that "[t]here has been extensive analysis of distinct writing styles, sayings, spelling mistakes, cliches and specific nuances, which have led to determining ATHAVALE as *a highly likeable target*." *Id.* (emphasis added). Also, HSI O'Hare formally requested the assistance of HSI Vancouver (where Mr. Athavale reportedly resided) in the investigation of Mr. Athavale. *Id.*

In another report regarding Mr. Athavale, SA Der-Yeghiayan set forth in six pages of detail, with specific examples, 27 separate similarities "in use of words or statements" made by Mr. Athavale and DPR. 3505-3072-78, as well as lengthy passages from posts made Mr. Athavale. 3505-3078-83.

The government's attempts, in its Memo of Law, at 18, to minimize the importance of SA Der Yeghiayan analysis of language patterns in identifying DPR would be merely unavailing if they were not so disingenuous and contrary to the government's professed investigative purposes with respect to Mr. Ulbricht.

For example, the warrant for Mr. Ulbricht's laptop (attached as Exhibit 11 to the August 1, 2014, Affidavit of Joshua L. Dratel, Esq., in support of Mr. Ulbricht's motion to suppress certain evidence) sought, and received, authorization to search for precisely that information:

> 44. The SUBJECT COMPUTER is also likely to contain evidence concerning ULBRICHT relevant to the investigation of the SUBJECT OFFENSES, including evidence relevant to corroborating the identification of ULBRICHT as the Silk Road user "Dread Pirate Roberts," including but not limited to:
>
> a. any communications or writings by Ulbricht, which may reflect linguistic patterns or idiosyncracies associated with "Dread Pirate Roberts"[] or political/economic views associated with "Dread Pirate Roberts" *(e.g.,* views associated with the Mises Institute);
>
> * * *
>
> c. any evidence concerning Ulbricht's travel or patterns of movement, to allow comparison with patterns of online activity of "Dread Pirate Roberts" and any information known about his location at particular times;
>
> * * *
>
> h. any other evidence implicating ULBRICHT in the SUBJECT OFFENSES.

See ¶ 44 of the Application for a Search Warrant for Mr. Ulbricht's laptop.

The footnote to ¶ 44(a) explained the basis for that blanket search:

> For example, "Dread Pirate Roberts" is known often to begin sentences with "Yea" – distinct from the usual spelling of the word, "Yeah." ULBRICHT is also known to favor this spelling of the word; for instance, his username on YouTube is "ohyeaross." The SUBJECT PREMISES is expected to contain writings or communications that will allow for similar linguistic comparisons between ULBRICHT and "Dread Pirate Roberts."

Id., at ¶ 44(a) n. 21.

In fact, the government prepared (but did not use) for SA Der-Yeghiayan's re-direct examination at trial a series of exhibits highlighting, with red circles, that alleged idiosyncracy in various electronic communications. Thus, again, the government's argument is contradicted dispositively by its own investigative priorities and its trial preparation.

Thus, SA Der-Yeghiayan devoted countless hours examining Mr. Athavale's language patterns, and ultimately a series of pages in his reports to the subject, and even submitted all the material to a college professor for expert analysis, with the professor reporting back that Mr. Athavale and DPR "could very well be the same person." 3505-317.

It is assumed, based on the search warrant application for Mr. Ulbricht's laptop and social media accounts, as well as the prospective government exhibits at trial, that SA Der-Yeghiayan and/or other agents and AUSA's performed the same meticulous scrutiny with respect to Mr. Ulbricht's communications. Yet no such opinion by a college professor or anyone else was provided to the defense with respect to Mr. Ulbricht.

Moreover, SA Der-Yeghiayan's interest in Mr. Athavale remained active until at least April 2013 – well after former SA Force, in his guise as DeathFromAbove, had alerted DPR that the government believed he was Mr. Athavale – as evidenced by subsequent e-mails from SA

Der-Yeghiayan. *See* 3505-3057-58 (e-mails dated April 3, 2013 & April 4, 2013).

Thus, Mr. Athavale represented not a "hunch" or "lead," but rather, as described by the Special Agent with the most law enforcement experience monitoring and studying the Silk Road website, was "a highly likeable target" to whom significant investigative resources were devoted, including numerous hours of SA Der-Yeghiayan's time, for at least five months. It bears noting as well that, as is the case with Mr. Karpeles, the government has never examined Mr. Athavale's electronic devices or his e-mail accounts, or the contents of the various servers and internet domains he has controlled. T. 682.

Judge Alex Kozinski, dissenting in *United States v. Olsen*, 737 F.3d 625 (9th Cir. 2013), announced that "[t]here is an epidemic of *Brady* violations abroad in the land[,]" and that "[o]nly judges can put a stop to it." *Id*., at 626 (Kozinski, J., *dissenting*). *See also id*., at 631-32 ("*Brady* violations have reached epidemic proportions in recent years, and the federal and state reporters bear testament to this unsettling trend") (citations omitted).

Judge Kozinski added that "[a] robust and rigorously enforced *Brady* rule is imperative because all the incentives prosecutors confront encourage them not to discover or disclose exculpatory evidence . . ." *Id*., at 630. As a result, Judge Kozinski urged his judicial colleagues that they "must send prosecutors a clear message: Betray *Brady*, give short shrift to *Giglio*, and you will lose your ill-gotten conviction." *Id*., at 633.

D. ***The Information That Was Not Disclosed Until the Force Complaint Was Unsealed***

The Force Complaint also revealed information that was not previously disclosed by the government. Obviously, the most dramatic was the involvement of a second law enforcement agent, former SA Bridges, in the corrupting of the Silk Road investigation. However, there were

other revelations, in both kind and degree, that appeared for the first time in the Force Complaint, but which should have been disclosed to the defense herein earlier, and even before trial.

As discussed **ante**, the investigation of former SA Bridges was already fully underway by Fall 2014, and his misconduct, was known by then as well (as demonstrated by the contents of the interviews of him). Former SA Bridges's relevance to this case is beyond obvious: as the Force Complaint attests, former SA Bridges "had been assigned to the Secret Service's Electronic Crimes Task Force." Force Complaint, at 40. Also, former SA Bridges's "specialty was in computer forensics and anonymity software derived from TOR." *Id.* Former SA Bridges was also "the Task Force's subject matter expert in Bitcoin." *Id.*

Beyond his particular expertise, firmly in the wheelhouse of multiple critical aspects of this case (computer forensics, TOR, and Bitcoin), former SA Bridges placed himself firmly in the middle of important factual issues, such as his serving as the affiant for the seizure of Mark Karpeles's Dwolla accounts in May 2013. *Id.*, at 41. Former SA Bridges also, according to the Force Complaint, served as the affiant for other documents. *Id.*, at 41.

In addition, former SA Bridges clearly worked in concert with former SA Force. *Id.*, at 43, 45. Thus, former SA Force was assisted in his illegal, unauthorized infiltration and manipulation of the Silk Road website by a computer forensics with expertise in anonymity and Bitcoin. Yet none of this information was disclosed to the defense herein until the filing of the Force Complaint. Clearly, the government at some point and in some fashion abandoned its "abundance of caution" policy altogether.

The timing, volume, and sophistication of former SA Force's Bitcoin transactions were

also provided for the first time in the Complaint. *See* Force Complaint, at 4 (former SA Force "engaged in a series of complex transactions between various Bitcoin accounts . . ."). Former SA Force received "several large international and domestic wire and Automated Clearing House (ACH) transfers through the latter half of 2013 and first half of 2014." *Id.*, at 7.

Former SA Force's deposits totaled at least approximately $757,000 "for the roughly year long period beginning April 2013 through May 2014." *Id.*, at 7-8 (footnote omitted). Nor does that include other deposits made afterward. *Id.*, at 8 n. 2. Any deposits made in the first half of 2014 would of course have occurred *after* Mr. Ulbricht had been arrested, begging the question of the source of those funds.[8]

The Force Complaint also divulged former SA Force's additional misconduct, which sheds light on his capacity for fraud, deception, forgery, abuse of his government authority and access – including predatory and retaliatory conduct and false accusations against innocent persons – and inventing complex, layered cover stories to conceal his misdeeds.

For example, the Force Complaint, at 29-33, in a section entitled "FORCE's Unlawful Seizure of R.P.'s Funds," details former SA Force's series of attempts to convert the contents of an account held by "R.P.," which efforts included abuse of various criminal law enforcement

---

[8] Regarding the value of the Bitcoins former SA Force received via Silk Road, the Complaint notes how those quantities could be leveraged into extraordinary sums depending on when they were exchanged, *see* Force Complaint, at 15 & n. 8, (a concept the government resisted at trial but now embraces) with the maximum value reached soon after Mr. Ulbricht's arrest, a time – perhaps not coincidentally, when former SA Force attempted to cash out. *See Id.* ("during the time FORCE was liquidating bitcoins through his own personal accounts, the value of bitcoin fluctuated dramatically ranging from less than $300 per bitcoin to over $1100 per bitcoin"). *See also id.*, at 43 n. 26 (at its peak value in Fall 2013, the 20,000 bitcoins delivered January 25, 2013, from Silk Road accounts to a bitcoin wallet address would have been worth "in excess of $20 million").

privileges and false accusations against "R.P." to justify seizure of the account.

Former SA Force also misused subpoenas and in effect committed forgery by using his supervisor's stamp. *See id.*, at 29, 33-34, 35. *See also id.*, at 4 (former SA Force "used his supervisor's signature stamp, without authorization, on an official U.S. Department of Justice subpoena and sent the subpoena to a payments company, Venmo, directing the company to unfreeze his own personal account"). He also improperly performed queries in law enforcement criminal databases. *See* Force Complaint, at 27.

Moreover, former SA Force "'papered up' the seizure of the digital currency portion of" one of his victim's accounts "in such a way that he may have thought he would be covered in the event anyone ever asked any questions" about his conduct." At 32. *See also id.*, at 33 (former SA Force's documentation was an "attempt to give himself plausible deniability by memorializing the digital currency seizure . . .").

Thus, the extent and in some respects the nature of former SA Force's misconduct – as well as former SA Bridges's participation altogether – was hidden by the government from the defense in this case until well after trial.

E. ***What Remains Unknown (to the Defense, At Least) About SA Force's and Bridges's Misconduct In the Context of the Silk Road Investigation***

Nor can the government state the extent of that misconduct, which raises additional questions about what remains unknown. In fact, the government – even in the Force Complaint, or in any other context – cannot confirm the full range of former SA's Force and Bridges's misconduct and illegal activities in connection with the Silk Road site and investigation. Nor can the government produce or confirm the full range of communications and/or relationship between former SA's Force and Bridges with Dread Pirate Roberts, or any other person or entity

involved in the Silk Road site.

In fact, as the Force Complaint acknowledges with respect to the contacts between former SA Force and DPR, "[m]any but not all of their communications were encrypted[.]" *Id.*, at 12. Also, while "[s]ome portion of the communications between DPR and Nob (FORCE) are memorialized in FORCE's official case file . . ." and "[s]ome of the communications are also preserved on FORCE's official computers[,]" nevertheless "not all of the communications between DPR and Nob (FORCE) were memorialized." *Id.*, at 12.

Nor did former SA Force memorialize in any government file or computer his private key necessary to decrypt those PGP-generated communications with DPR. As a result, as the Complaint notes, the government cannot even provide a full account of former SA Force's communications with DPR. *Id.*, at 13-14. The Force Complaint also concluded that the encryption and failure to memorialize the private key was indicative of former SA Force's intent to conceal those communications from the government and that the reason was because they were corrupt communications. *Id.*, at 13-14. *See also id.*, at 13 ("the communications should have been documented, in deciphered form, and memorialized in the file").

The encrypted communications grew in frequency as the relationship between former SA Force and DPR progressed: "toward the end of the timeframe in which Nob (FORCE) was in relatively heavy communication with DPR, FORCE increasingly was not providing the decrypted versions of their communication." *Id.*, at 14.

For instance, for the chain of messages between former SA Force and DPR from July 31, 2013, through August 4, 2013, all but one of the messages (which was from DPR) are completely encrypted. *Id.*, at 16. Also, the communications between French Maid (another of

former SA Force's aliases)[9] and DPR, spanning from August 26, 2013, through September 13, 2013, were also predominantly encrypted. *See* Force Complaint, at 21. However, the Force Complaint tells only part of the encryption story, as review of discovery establishes that the range of Nob's encrypted communications with DPR was from January 29, 2013, through August 4, 2013.

As evidence of some of the encrypted communications between former SA Force and DPR, the Force Complaint also cites the portions included in the "LE_counterintel" file (proposed Defendant's Exhibit C at trial in this case) found on Mr. Ulbricht's laptop, which file, in response to government objections discussed in a sealed robing room conference prior to court February 3, 2015, the defense was permitted only to summarize – and only portions thereof (despite the defense's request to admit the entire document and/or read from additional sections). *See also* Force Complaint, at 20 ("the file appears to contain cut and pasted sections of what the insiders were relaying to [DPR] through online chats or private messages."

Yet the Complaint acknowledges the importance of that LE_counterintel file: "[p]rior to his arrest, DPR was known to have been hiding his true identity and location from law enforcement, so information concerning the government's investigation was material and valuable to him." *Id.*, at 13.

Also, the government cannot provide any assurance that *all* of former SA Force's communications with DPR – regardless of the particular alias utilized by former SA Force –

---

[9] Interestingly, the Force Complaint cites as one basis for identifying former SA Force as French Maid their mutual use of an outdated version of software, the same technique used by SA Der-Yeghiayan with respect to Mr. Karpeles and the use of an outdated version of MediaWiki software. T. 659-63 (January 20, 2015).

have been preserved in *any* form, even encrypted. Nor is there any certainty with respect to how many aliases former SA Force employed – indeed, it was not until the defense pointed it out at trial that the government realized Death From Above was one of those aliases – or with whom he communicated with respect to Silk Road (via any system, *i.e.*, Silk Road Forum, private messaging, Tor chat, Pidgin chat).

Also unknown is the precise extent of former SA's Force and Bridges's compromising of the Silk Road website. In its Memo of Law, at 12 n. 3, the government provides bullet point arguments why what it describes as a defense "scenario was implausible . . ." Of course, no SDNY AUSA has ever described any defense as "plausible," but in any event that is an argument with respect to the *weight* of the evidence, an issue for the jury.

Nor are the government's arguments persuasive in any event. The codebase for the Silk Road site, PHP myadmin,[10] provided in discovery reveals that an administrator with the level of access granted to the user "Flush" could have reset the PIN on DPR's account and usurped control of it. Indeed, at the December 15, 2014, pretrial conference (previously sealed portion), the government could not state for certain what level of access former SA Force possessed as a result of his corrupt activities. *See* Transcript, December 15, 2014, at 40-43.

With PHP myadmin access, Flush (whose account former SA Force initially hijacked), or anyone (such as former SA's Force and/or Bridges) could have changed anything in the Silk Road database, including message text in the Forum or Market messages, and re-set passwords. There were multiple PHP myadmin accounts; therefore, Flush (or someone acting as him) could have had access to DPR's account without DPR losing access.

---

[10] PHP is a server-side scripting language and can be used to build web applications.

In addition, the second SSH key – to which government witness Brian Shaw testified to at trial, *see* T. 1970-71 (February 2, 2015), unquestionably provided root access to the Silk Road server(s), and it is unknown who had access via that SSH key, or when it was created. Mr. Shaw did testify, however, that the "Frosty" SSH key was modified March 26, 2013, certainly after former SA's Force and Bridges's corrupt access to the Silk Road site.

Also, in a TOR chat log commencing February 17, 2012, at 19:14, DPR and Inigo (another administrator for the Silk Road site), there is discussion for approximately half an hour regarding privileges provided to Inigo for access to the Silk Road *database*. It is unclear whether Flush was granted the same access, but certainly the government has not established that Flush did not enjoy such access. In addition, the government's contention about the private key is meritless, as that key could easily have been duplicated.

Absent the opportunity to inspect items relevant to the investigation of former SA's Force and Bridges, the full extent of potentially exculpatory material cannot be determined. At this point, the defense has only a limited idea of the extent to which former SA's Force and Bridges were able to penetrate the Silk Road site given their level of administrative access. From information publicly available about the investigation, though, it appears that certainly former SA Bridges, and even former SA Force, had a relatively high level of technical sophistication. It is feasible that given their level of access, former SA's Force and Bridges could have been able to exploit vulnerabilities in the site to gain access to other administrative accounts, or possibly even the Dread Pirate Roberts account.

In that context, if the defense theory was "implausible," there was certainly no harm in its admission at trial. Rather, the government's still feverish efforts to preclude presentation of that

evidence demonstrates that it was material to the trial. Moreover, the information regarding former SA's Force and Bridges cannot be viewed in isolation. Instead, it must be evaluated along with other evidence the defense introduced at trial, and which it offered but was denied admission. Taken together, that evidence provides a compelling defense that Mr. Ulbricht should have been allowed to present to the jury.

Another still unknown aspect is the contents of the still-sealed paragraph (at 11) in the Force Complaint. In addition, the Force Complaint itself notes that it "does not include certain additional facts known to me and the government's investigation continues." *Id.*, at 6.

F. *The Record Demonstrates That Silk Road Investigations Were Coordinated and, for Practical Purposes and for Determining Relevance to This Case, Combined*

The government's repeated insistence that the Southern District of New York's investigation was "independent" of that in which former SA's Force and Bridges were involved is demonstrably repudiated by the record *created by the government's investigators and prosecutors themselves*.

That record establishes that all of the federal investigations of the Silk Road website, were coordinated and, for practical purposes, combined. To the extent there is any question with respect to that conclusion, it is respectfully submitted that the Court should order and conduct an evidentiary hearing on the issue.

By any conception of "independence," these investigations do not qualify. Rather, they were decidedly *inter*dependent because, as detailed below,

- the agents conducting the investigation were in continued contact with each other regarding the status of the investigations;
- supervisory law enforcement officials coordinated the investigations;

- each investigation made its fruits available to the other, and used that information from the companion investigation(s);
- information was entered in law enforcement databases to which all federal law enforcement enjoyed access;
- the investigations sought information about and from the same targets at the same time; and
- ultimately, SDNY was able to dictate the distribution of federal charges in the case for *all* of the districts involved in the coordinated investigations.

The 3500 material produced for SA Der-Yeghiayan serves as a catalogue of the interaction and linkage of the various investigations of the Silk Road website. For example, a report by SA Der-Yeghiayan regarding his investigation of Mr. Athavale (discussed in more depth **ante**, at 26-30), notes that in October 2012, "HSI Baltimore office provided SA Der-Yeghiayan with a file containing all of the Undercover (UC) chats made between a UC agent and DPR." 3505-3072 (attached hereto as part of Exhibit 4).

Similarly, in a May 22, 2013, e-mail to Lisa M. Noel, an HSI intelligence analyst with HSI Baltimore (and part of that Silk Road Task Force), SA Der-Yeghiayan wrote that "[w]e would like to examine some of the language, usage, diction, etc. with the new U/C chats from Nob." 3505-628. *See also* 3505-630 (in a November 2, 2012, e-mail regarding analyzing Mr. Karpeles's writing, SA Der-Yeghiayan remarks that "[t]his professor knows dread's writing better than anyone, it would be good to show him raw posts that are unedited").

Thus, at the outset of his investigation – which the government cannot claim was "independent" of the case against Mr. Ulbricht – SA Der-Yeghiayan was provided with the

principal product of the Baltimore investigation, *generated by former SA Force himself*. Thus, the connection is inescapable, regardless of the government's mantra of "independence."

Other e-mails and reports authored by SA Der-Yeghiayan describe the continued contacts. In a May 15, 2013, e-mail, SA Der-Yeghiayan wrote that "[i]n early August 2012, HSI Chicago notified HSI Baltimore of the connection made [between Mr. Karpeles and Silk Road] and stated that Karpeles was a target of HSI Chicago's investigation." 3505-273. Also, "HSI Baltimore was provided a copy of the HSI Chicago's ROI [Report of Investigation] that highlighted all the facts of the connection." *Id.*

In that same e-mail, SA Der-Yeghiayan memorialized the following interaction:

> HSI Chicago contacted HSI Baltimore and they confirmed that they shared all of HSI Chicago's information on KARPELES with members of their task force. HSI Chicago discovered that their IRS Agent, DEA Agent and SS Agent all inputted KARPELES into their individual investigations as a target and a potential administrator of the Silk Road based on HSI Chicago's ROI/information.

Id.

Subsequently, in an undated report, at 3505-273-75 (attached hereto as Exhibit 5), SA Der-Yeghiayan provided the following chronology:

- "[o]n May 10, 2013, [SA Der-Yeghiayan] was contacted by the HSI case agent and the Baltimore AUSA that the SS agent in their task force had issued a civil seizure warrant for Mutum Sigillum's Wells Fargo bank account. Both the case agent and AUSA stated they were not notified by the SS agent in their task force of the seizure warrant before it was already filed. The AUSA stated that he learned that the SS headquarters was notified that Wells Fargo had closed down

Mutum Sigillum account over suspicions of [18 U.S.C. §]1960 violations and the money was going to be returned to KARPELES. It is not exactly known at this time, but HSI Chicago believes that SS Headquarters notified the SS agent in Baltimore based on his record on KARPELES and therefore he got involved in making the seizure." 3505-274;

- "[t]he following Monday May 13, 2013, HSI Baltimore and the Baltimore AUSA Justin Herring contacted HSA Chicago to notify him that they negotiated with SS Baltimore to seize the money in KARPELES's Dwolla account using the same affidavit written by the SS. The total in the account was said to be over 3 million USD. HSI Baltimore stated that they would add Chicago's project code for their CUC and case number to their seizure of 3 million." 3505-275;
- "[t]he Chicago AUSA Marc Krickbaum is aware of both seizures and has informed the AUSA Justin Herring in Baltimore that Chicago was still intending on possibly pursuing criminal charges for 1960 violations that occurred in the State of Illinois. AUSA Marc Krickbaum had no objections to the SS seizure or HSI's seizure over the accounts even though HSI Chicago felt they should be making the seizure on the Dwolla account." *Id.*;
- "[i]t is HSI Chicago's and HSI Baltimore's case agent's position that the SS Baltimore Agent would never have been alerted by SS headquarters about KARPELES's bank account had it not been for the record they entered as a direct result of it being provided to them by HSI Chicago through HSI Baltimore. HSI Chicago is the source of the information for Baltimore's work on KARPELES as

well. HSI Chicago maintains the longest standing TECS records on KARPELES, and exclusive TECS records on Mt. Gox and Mutum Sigillum." *Id.*;

- "[c]ase agent Jared Der-Yeghiayan is also of the opinion that HSI Baltimore should have offered to defer the Dwolla seizure of 3 million USD plus to HSI Chicago knowing that they had developed the charges in their district and were pursuing criminal charges." *Id.*

Another, (seven-page) report from SA Der-Yeghiayan regarding various investigations into Silk Road further recounts their interlocking character. 3505-295-301 (attached hereto as Exhibit 6). For example,

- January 13, 2012, a Baltimore HSI supervisor "requested a phone call about HSI Chicago's Silk Road case." 3505-295;
- February 1, 2012, representatives of HSI Baltimore flew to Chicago for a meeting regarding the Silk Road investigation. AUSA's from both jurisdictions attended, as did HSI case agents and other personnel (including an Intelligence Analyst). *Id.*;
- during that February 1, 2012, meeting, HSI Baltimore "requested to split up our investigation so they could work a section of it[,]" to which HSI Chicago "strongly disagreed and stated that they were fully advance[d] in the case and did not see any advantage to give up any aspect of their investigation which included the administrators and organizers." *Id.*;
- HSI Baltimore claimed to have an informant who would enable HSI Baltimore to "take down the site within a week or two with that information." HSI Chicago

"disagreed that could be done and disagreed with the strategy they intended to take and stated they were working all aspects of the investigation and wanted to send a message with the case." 3505-296;

- "[t]he [February 1, 2012] meeting ended with HSI Baltimore stating that they intended on shutting down the website soon and weren't concerned with HSI Chicago's stragegy but they would coordinate once they take the website down." *Id.*;
- communications between HSI Chicago and HSI Baltimore continued with respect to the status of the investigation of Silk Road. *Id.*;
- in April 2012, HSI Chicago developed a new informant and informed HSI Baltimore. According to SA Der-Yeghiayan's report, "HSI Baltimore requested access directly to the informant but wouldn't tell HSI Chicago why they wanted access or what they wanted to ask the CI [Confidential Informant]. HSI Chicago offered to take any questions and directly ask the CI the questions for them, but they would not allow access to the CI without knowing any topic of questions. HSI Baltimore expressed anger over not being allowed direct access to the CI." *Id.*;
- in July 2012, HSI Chicago identified Mark Karpeles as a target of the investigation, and entered a record to that effect in the TECS system, to which all federal law enforcement agencies have access. 3505-296-97;
- July 9, 2012, a Baltimore HSI agent "wanted to send out a draft for HSI Headquarters notifying all HSI offices that he is the POC [point of contact] for all

Domestic Silk Road related investigations and that HSI Chicago will be the POC for all international related investigations. HSI rewrote HSI Baltimore's draft to state that they were [either redacted or missing]." 3505-297;

- during July 2012, more inquiries arose with respect to coordinating the HSI Chicago and HSI Baltimore investigations of the Silk Road website (*id.*);
- August 3, 2012, [HSI supervisory officials] informed SA Der-Yeghiayan that they believed HSI Baltimore wanted funding to travel to the foreign country to interview [Mr. Karpeles]." In response, SA Der-Yeghiayan sent an e-mail to HSI Baltimore agents "notifying them that [Mr. Karpeles] was more involved in the Silk Road and was a target o[f] their invesigation, and asked in the email not to share the information with the rest of their unofficial Task Force." *Id.*;
- August 23, 2012, "HSI Chicago was called to a meeting at [HSI supervisory offices] to meet with HSI Baltimore and each present their cases to both SACs [Special Agent in Charge] Operations each of their cases. At the end of the presentations both HSI Baltimore and HSI Chicago's Operations Managers were discussing the confusion and odd approach to the HSI Baltimore's investigation and asked HSI Chicago if [HSI Baltimore's] investigative methods are interfering with HSI Chicago's case. HSI Chicago expressed deep concern for HSI Baltimore's tactics and the lack of focus in their investigation." *Id.*;
- in October 2012, an HSI Baltimore agent "began asking SA Der-Yeghiayan for all his information on [Mr. Karpeles] because they were trying to work him too. In response, SA Der-Yeghiayan "informed [the HSI Baltimore agent] to not work

[Mr. Karpeles] independent of HSI Chicago." 3505-298;

- "HSI Chicago later discovered that HSI Baltimore had disseminated [Mr. Karpeles] to all members of their task force and they had issued multiple subpoenas on [Mr. Karpeles], and actively worked him to include a type of surveillance without the knowledge of HSI Chicago." *Id.*;
- "[i]n early October 2012, HSI Chicago began developing a method to identify the main administrator of the website by analyzing thousands of pages of text on various websites to make a match. In early November 2012, HSI Baltimore offered to provide UC [Under Cover] Chat information with the administrator to help HSI Chicago with their development. HSI later identified a target [Anand Athavale] and began issuing subpoenas to further the identification and location of [Mr. Athavale]. HSI Chicago informed HSI Baltimore and shared the subpoena information with HSI Baltimore." *Id.*;
- in December 2012, HSI Baltimore continued to request from HSI Chicago information regarding Mr. Karpeles. 3505-299. In late April 2013, "HSI Baltimore stated that they had looked heavily on their own into [Mr. Karpeles] and don't believe [Mr. Karpeles] is involved in the website no longer. HSI shared a few of their subpoena returns they received in early May." *Id.*;
- May 10, 2013, "[HSI] Baltimore notified HSI Chicago that the SS agent in their Task Force went 'rogue' and seized the bank account in the U.S. containing 2

million dollars from [Mr. Karpeles].[11] HSI Baltimore claimed to have no knowledge of the seizure until after it occurred. HSI Baltimore also admitted that they told the SS agent of the connections HSI Chicago made to the Silk Road back in August of 2012. HSI Baltimore stated that the SS agent went to a totally different AUSA in their District to file the affidavit to seize the account." *Id.*;[12]

- May 13, 2013, "HSI Baltimore called HSI Chicago and stated that they had complained enough to the SS about the way the agent went behind their back that the SS agreed to give HSI the other account containing 3 million USD belonging to [Mr. Karpeles]. HSI Baltimore proceeded to ask HSI Chicago if they could provide any other bank accounts belonging to [Mr. Karpeles] so they could seize those accounts too. HSI Baltimore proceeded to seize the 3 million USD using the same affidavit written by the SS agent except [the HSI Baltimore agent] substituted his name and knowing that HSI Chicago built their pending charges [against Mr. Karpeles] on those seizures." *Id.*;[13]

---

[11] As the Force Complaint states, May 9, 2013, former SA Bridges "served as the affiant on a multi-million dollar seizure warrant for Mt. Gox and its owner's bank accounts" two days after receiving a large wire transfer from Mt. Gox and benefitting in the amount of $820,000 fronm a Mt. Gox account. Force Complaint, at 5. *See also id.*, at 9, 45.

[12] Despite the concentration on this issue during cross-examination of SA Der-Yeghiayan, and the government's related motion to preclude cross-examination and strike testimony, the government remained inexplicably mum regarding its knowledge of former SA Bridges's role in securing that seizure affidavit. If there is any question regarding what the government knew and when it knew it, it is respectfully submitted that the Court should order and conduct an evidentiary hearing on the issue.

[13] While HSI Chicago had expressed its intention to seek charges against Mr. Karpeles for violating 18 U.S.C. §1960 (operating an unlicensed money service business), HSI Baltimore had decided it would not pursue such charges. 3505-298.

- during a May 17, 2013, conference call that included as participants an AUSA from the Northern District of Illinois, two AUSA's from the District of Maryland, and HSI agents from both HSI Chicago and HSI Baltimore, one of the D.Md. AUSA's "stated they were trying to work on an interview with [Mr. Karpeles] with [Mr. Karpeles's] attorneys." The N.D. Illinois AUSA "asked what the purpose of the interviews was and [the D.Md. AUSA] stated they wanted to know more about [Mr. Karpeles's] money business and wanted to ask him directly about his knowledge of the Silk Road." In response, "HSI Chicago expressed serious concern over that approach and was concerned as to [the D.Md. AUSA's] using HSI Chicago's information developed on [Mr. Karpeles] for their own use." Ultimately, the "outcome of the" conference call was that one of the D.Md. [3505-299-300;
- HSI Chicago and HSI Baltimore conducted a "joint" search warrant "based on a new target developed by HSI Chicago." 3505-300;
- HSI Chicago and HSI Baltimore conducted another conference call July 9, 2013, about the Silk Road investigation. *Id.* During that call, neither the HSI Baltimore agents nor the D.Md. AUSA on the call mentioned – despite a question from SA Der-Yeghiayan whether there were any new developments – that another D.Md. AUSA had scheduled a meeting with Mr. Karpeles's attorneys. *Id.* That meeting occurred July 11, 2013. *Id.* During the meeting, Mr. Karpeles's attorney "randomly brought up the Silk Road and stated that their client was willing to tell them who [Mr. Karpeles] suspects is currently running the website in order to

relieve their client of any potential charges for [18 U.S.C. §1960]." *Id.* Also, the D.Md. AUSA "proceeds to set up a meeting with [Mr. Karpeles] overseas." *Id.* HSI Chicago did not learn of the July 11, 2013, meeting with Mr. Karpeles's attorneys until July 16, 2013. *Id.* Subsequently, one of the D.Md. AUSA's informed SA Der-Yeghiayan that the other D.Md. AUSA "continued to negotiate with [Mr. Karpeles's] attorneys" – despite SA Der-Yeghiayan's objections – and has changed the meeting location to Guam [] later on in August. *Id.*;

- July 12, 2013, there was a "coordination meeting with HSI Chicago, HSI Baltimore, *FBI New York* and multiple DoJ [Department of Justice] attorneys and CCSIP attorneys[.]" 3505-300. At that "coordination meeting, "HSI Chicago mentioned [Mr. Karpeles] as their main target." *Id.*;

A month later, in August 2013, SA Der-Yeghiayan swore to the affidavit, composed by AUSA Turner, in support of the SDNY search warrant application for Mr. Karpeles's e-mail accounts. Again, in light of this overwhelming evidence, any claim of "independence" is untenable. In the event there remains any question, it is respectfully submitted that an evidentiary hearing is necessary to challenge the government's utterly unreliable and unsupported assertions (that are contradicted by the government's own documents).[14]

Nor was former SA Force's investigation into Silk Road was transitory or superficial in any respect. It began in February 2012, *see* Force Complaint, at 22 n.14, and generated dozens of DEA-6 reports of his (authorized) undercover activities investigating the Silk Road website.

[14] A separate question that merits an answer is whether any evidence related to Nob or Flush was introduced in the grand jury that indicted Mr. Ulbricht.

In fact, as the Force Complaint points out, information-sharing, and its impact relevant to this case, continued through the summer of 2013: "by late July 2013, the Baltimore Silk Road Task Force had been made aware that the FBI was seeking to obtain an image of the Silk Road server, and therefore FORCE may have had reason to fear that any communications between himself and DPR would be accessible to the FBI in the event the FBI was successful in imaging the server." Force Complaint, at 17-18.[15]

Even the government's Memo of Law, at 14 n. 4, contradicts its naked claim of "independence." That footnote, in explaining the government's realization (after the defense attempted to introduce certain documents provided in discovery) that DeathFromAbove was among former SA Force's aliases, states that "former SA Force had access to law enforcement reports filed by SA Der-Yeghiayan, including reports concerning his suspicions regarding Anand Athavale, which was likely the source of the information leaked by Force through the "DeathFromAbove" account." (Citation omitted).

Ultimately, the investigations were not only interrelated and interdependent, but their outcomes were dictated by SDNY. As SA Der-Yeghiayan reported in a September 20, 2013, e-mail to an HSI colleague,

---

[15] That would also ostensibly have provided DPR, via former SA Force as Nob (or French Maid, or alpacino, or DeathFromAbove, or perhaps some other incarnation) with advance notice of the FBI's imaging of Silk Road's servers – consistent with the defense's position that DPR purchased and/or was provided with information that permitted him to formulate and implement – with former SA Force's (and perhaps former SA Bridges's) assistance – an escape plan that also incriminated Mr. Ulbricht falsely. In that context, former SA Force also learned at least days in advance that law enforcement intended to make an arrest of DPR in late September 2013, thereby giving him ample time to warn DPR. *See* Force Complaint, at 18 & n. 10. Yet Mr. Ulbricht did not assume any additional security protocols, but instead violated even the most fundamental security precepts in multiple ways.

> I think that would be a good pitch but that they can't expect to take an admin or something – they all need to be prosecuted out of the same AUSA's office under a conspiracy – NY will never agree to anything else. It's not like they can give them an admin, that makes no sense from a prosecutorial standpoint.
>
> Baltimore can have a few vendors of our choosing – as well as the ability to say they "helped" ID some of the admins by "allowing" NY to use OUR UC account to identify some of the lower admins, and they can have sloppy seconds on DPR for their murder for hire. They can also have some info on other bitcoin companies that MK might name is shady after we get done with him.
>
> That's the best that can be given and they should consider themselves lucky for getting anything close to that. Or we can just stall, and Baltimore gets nothing and we contributed to the other two admins getting away [redacted]. We'll get no HSI banner on the site, and will probably get no cooperation from NY with any information related to MK. If DPR names MK in the interview and we didn't help them get the other admins when we had the chance – NY will leave us out of it and tie him into their conspiracy. We will then be left dealing with HSI Baltimore's tears and them then trying to take [redacted].
>
> I think it's important we help them have a "come to Jesus" moment otherwise our agency loses as a whole. It's a simple sell if they know the alternative is they will be left with absolutely nothing – no matter how much they whine and complain to HSI HQ, it won't stop the SDNY from prosecuting all of them without any of us.

3505-319 (attached hereto as Exhibit 7).

A half-hour later that same day, September 20, 2013, SA Der-Yeghiayan e-mailed that same colleague with the following message:

> I think there's room to avoid the drama by instead of dwelling on the past or trying fluff up each others cases under the false assumption that the website will be up in the next month to talking about how to try and make HSI in general walk away from this without looking like complete fools. But it has to start with HSI Baltimore conceding that they will not be identifying or prosecuting dread first or any other admin for a fact. Then realizing that they still stand a chance, if they play nice, to walk away from this with something to show from their "investigation."

> They can easily erase a lot of the damage they've done by cooperating with NY's almost guaranteed prosecution of the website.
>
> The only two options are remain in denial and walk away with nothing but blame and egg on their face in the next few weeks, OR play nice and possibly take some credit for the identification and prosecution of all the admins, and reap some of the benefits by prosecuting some of the vendors our defendant is going to identify. No other way forward than that.

3505-320 (attached hereto as Exhibit 7).

Thus, in light of all of the evidence set forth above, the interdependence and continuing relationship among the investigations, including that in which former SA's Force and Bridges participated, is indisputable.

G. *The Information Regarding the Investigation of Former SA's Force and Bridges Would Be Relevant to This Case Regardless Whether the Investigations Were Independent*

Even assuming *arguendo* the SDNY investigation was "independent" from the District of Maryland investigation, the information and material regarding former SA's Force and Bridges was, *as evidenced by the government's own strategy in preparing for trial herein*, as well as other objective indicia, plainly relevant to this case.

1. *The Government's Initial Exhibit List*

The government's initial Exhibit List was provided December 3, 2014 – two days *after* the government's November 21, 2014, letter to the Court setting forth information regarding the investigation of former SA Force was disclosed to the defense – included a number of documents and materials directly relevant to former SA Force. For example,

- GX 220 was a Torchat buddy list that contained the identification for "Nob," an account operated by former SA Force;
- GX 225 was a Torchat between DPR and "Scout," dated January 26, 2013, in which DPR stated, "I'm not even going to hurt this guy that ripped me off if I can help it. This isn't the mob or cartel." Given the time frame of the chat, that is most likely a reference to "Flush," an account ultimately operated by former SA Force, and the administrator who was the subject of the alleged murder-for-hire scheme in which Nob was involved;
- GX 227 was a Torchat log between DPR and Cimon dated January 26, 2013, in which DPR stated, "had a csr go rogue and rip me off for 350k." That, too, related to the "Flush" account that ultimately was under former SA Force's control, and which he allegedly used to steal funds from the Silk Road website. The discussion also references Nob's involvement in the first alleged murder for hire plot;
- GX 229A was a Torchat log containing a conversation dated January 26, 2013, between DPR and PatHenry, in which, at 6, DPR stated "also I have Flush (our new guy) ready for you." That portion of the chat, however, was deleted from the exhibit ultimately entered into evidence at trial by the government as GX 229A;
- GX 229B was a Torchat log between DPR and Inigo containing multiple discussions regarding the "Flush" account, "Flush's" whereabouts, the money "Flush" had allegedly stolen from the Silk Road site, and as to his capture;
- GX 241 was the unredacted journal for part of 2013 recovered from Mr.

Ulbricht's laptop. The journal includes mid-September 2013, entries regarding DPR's communications with Silk Road user "French Maid," and April 2013 entries regarding DPR's communications with DeathFromAbove. Also, log entries for June 5, 2013, to September 11, 2013, made reference to "alpacino," another one of former SA's Force's unauthorized user accounts, who had been "leaking info to [DPR;]"

- GX 243 was the "LE_counterintel" file in its unredacted entirety. It included multiple entries regarding information provided by alpacino and by another source, "East India Traitor" (whose identity has been determined, at least by the defense, but who could be former SA Force as well). A copy of that proposed Government Exhibit, which was offered by the defense at trial as Defendant's Exhibit C, is attached hereto as Exhibit 8;
- GX 250 was a computer file entitled "SR_accounting," an alleged Silk Road expense report, that included references to "theft from mtgox" as well as regular payments to hackers and other extortionists, a large number of which occurred in the spring and summer of 2013;
- GX 252 was a document titled "todo_weekly.txt" which contained a section entitled "pay employees" that listed "albertpacino" as receiving $500 per week;
- GX 275 was a document entitled "ops.txt," and which was ultimately redacted to remove references to Curtis Green and his bitcoin address, both of which were related to the first alleged murder for hire plot involving former SA Force) by the government prior to its admission into evidence.

2. *The Government's Opposition to Mr. Ulbricht's Motion for Bail*

The government also relied on former SA Force's work in opposing Mr. Ulbricht's application for bail in November 2013. The government's November 20, 2013, letter included the following passages:

- "[t]he Complaint also describes how Ulbricht was willing to use violence to protect his online drug empire, commissioning multiple murders for hire in seeking to guard his interests in Silk Road. Ulbricht has been separately charged for one of these attempted murders for hire in an indictment issued by the United States Attorney's Office for the District of Maryland, unsealed on October 2, 2013." Gov't Letter, at 2. The government also attached the District of Maryland Indictment to its Response, as Exhibit B;
- "[m]oreover, he repeatedly resorted to violence in seeking to protect his lucrative business, commissioning at least six murders for hire in connection with operating the site." *Id.*, at 4;
- describing "no fewer than six murders for hire within a span of four months in 2013" that Mr. Ulbricht allegedly "commissioned," followed by a detailed account of the chats between DPR and Nob and others, and payment particulars. *Id.*, at 5; and
- describing another chat between Nob and DPR regarding DPR's concealment of his identity even from his girlfriend. *Id.*, at 10.

3. *The Importance of the First Half of 2013 Regarding the Evidence At Trial*

The relevance of the misconduct committed by former SA's Force and Bridges is also apparent from the time frame in which it is believed to have commenced and occurred – the first half of 2013. That period was critical in the context of the creation and collection of evidence used against Mr. Ulbricht at trial, and the defense's response to it.

A partial time line of relevant events during that span – described only by information possessed by the defense at the time of trial (and not including reference to former SA's Force or Bridges misconduct) – consists of the following:

- January 26, 2013: $350,000 is taken from Silk Road accounts;
- January 26, 2013: DPR learns "Flush" has been arrested for cocaine possession;
- January 26-29, 2013: DPR discusses a murder for hire plot with several Silk Road administrators, as well as with a federal law enforcement agent posing as a Silk Road user;
- February 2013: "Nob" murder for hire plot against Flush allegedly occurs;
- March 13, 2013: discussion thread regarding "friendlychemist" and "redandwhite" begins (GX 936);
- March 16, 2013: User with user name "Ross Ulbricht" posts a question on Stack Overflow (T. 1343-44 [January 28, 2015]);
- March 16, 2013: publicly displayed user name on Stack Overflow account changes from "Ross Ulbricht" to "frosty" (GX 1200; T. 1343-46[January 28, 2015]);
- March 21, 2013, March 25, 2013, and April 11, 2013: Silk Road servers are subject to a DDOS (distributed denial of service) attack (T. 928 [January 21, 2015]; T. 1443 [January 28, 2015]; T. 1755 [January 29, 2015]; *see also* GX 241]);

- March 26, 2013: SSH root access key to Silk Road servers modified to "frosty@frosty" (GX 901; T. 1753-1755 [January 29, 2015];

- March 31, 2013, April 8, 2013, and April 12, 2013: notable Bitcoin transactions occur those dates, as pointed out by SA Der-Yeghiayan in a September 16, 2013, e-mail (3505-355);

- April 1, 2013: communications to DPR from DeathFromAbove threatening DPR but also offering confidential law enforcement investigative information – including the name Anand Athavale as a government target – in exchange for payment begin (DX E);

- April 4, 2013: Email account associated with Stack Overflow account is changed from "rossulbricht@gmail.com" to "frosty@frosty.com" (T. 1347-48 [January 28, 2015]);

- April 15, 2013: murder for hire plot against "friendlychemist" allegedly carried out by "redandwhite" allegedly occurs, ending with a $500,000 payment (GX 936);

- May 10, 2013: HSI Baltimore seizes more than $2 million from accounts Mark Karpeles's company holds at Dwolla, thereby notifying Mr. Karpeles that he is on the government's radar (T. 729 [January 20, 2015]);

- Early June 2013: according to FBI Special Agent Christopher Tarbell, FBI first learns of the genuine IP address for the Silk Road servers (in Iceland) (*see* Declaration of former Special Agent Christopher Tarbell, at 3-4);[16]

- June 6, 2013: at the request of the U.S. government, law enforcement officials in Iceland image the Silk Road servers located there;

[16] The government, however, had a lead on a different Silk Road server months prior: "[s]everal months earlier, the FBI had developed a lead on a different server at the same Data Center in Iceland ("Server-1"), which resulted in an official request for similar assistance with respect to that server on February 28, 2013." *See* Tarbell Declaration, at 5 n.7.

- June 11, 2013: SA Der-Yeghiayan sends an e-mail noting the difficulty of determining the identities of users on the Silk Road site because multiple people were operating multiple accounts with different user names, leading him to ask, "Sheesh. Who's on first?" (3505-03523-03524; T. 426-28 [January 15, 2015]; T. 633-34 [January 20, 2015]);
- June 2013: "alpacino" begins providing DPR confidential law enforcement information in return for payment (DX D [which is the same as initial GX 241]);
- July 2013: DPR assumes control of the Cirrus/ Scout account to obtain information about Mr. Wonderful, allegedly a federal law enforcement agent who had been investigating DPR;
- July 11, 2013: HSI Baltimore agents meet with Mr. Karpeles's lawyers, who offer to reveal DPR's identity in exchange for the government not bringing any charges against Mr. Karpeles (3505-300; T. 490-556 [January 15, 2015]);[17] and
- July 23, 2013: FBI images the Silk Road servers located in Iceland.

4. *The Communications Between DeathFromAbove and DPR*

In foreclosing the defense's use of any information or materials relating to former SA Force and his misconduct, the government exceeded the boundaries set by the Court in its pretrial rulings on the issue. While the embargo was supposed to cover only the information and materials generated as part of the ongoing grand jury investigation of former SA Force, at trial in this case the government converted that into a ban on the defense's use of information and documents provided as part of discovery, which the defense had been expressly permitted to utilize at trial.

[17] The 3500 material discussed **ante**, at 25, relating how Mr. Karpeles's lawyers passed information about Mr. Ulbricht to the government, *see* 3505-2925, further connects the various investigations. Similarly, the interaction among investigations, and relevance to this case, is further established by the common mention of Mr. Athavale.

In fact, during the previously sealed portion of the December 15, 2014, pretrial conference, AUSA Turner, when asked by the Court about the parameters of the prohibition imposed on the defense by Rule 6(e), Fed.R.Crim.P., answered, "What they can't reveal is that [former SA Force] is under a grand jury investigation. . . . It's just a matter that he's being investigated for [certain activities]." Transcript, December 15, 2014, at 48.

AUSA Turner added that

> [s]o in terms of what [Rule] 6(e) prohibits, we think it prohibits them eliciting somehow that he's under a grand jury investigation. That's the basic point. I mean, that's what 6(e) requires be kept secret while the investigation is pending. They still have many facts in their possession. They've had them in their possession long ago.

Id.[18]

Yet the communications between DeathFromAbove and DPR were *not* mentioned in the government's November 21, 2014, letter to the Court, did not mention former SA Force at all, and did not disclose that he was under a grand jury investigation. Also, the government's reaction at trial to the defense's efforts to introduce those communications (as Defense Exhibit E, a copy of which is attached hereto as Exhibit 9), memorialized in the government's

---

[18] During the previously sealed portion of the December 15, 2014, pretrial conference, the Court recognized the government's inconsistent and expansive position with respect to the scope of the Rule 6(e) proscription. In response to AUSA Turner's remark that the "point is, we're not trying to say certain witnesses, certain evidence is off limits. It's the fact that this is a grand jury investigation. That's what they're prohibited from disclosing[,]" the Court replied

> [w]ell, I hear what you're saying. And it's like ships passing in the night. *Because on the one hand it's the content of the investigation*. And what you're suggesting is it's really not the content, it's the fact of.

Transcript, December 15, 2014, at 49-50 (emphasis added).

(previously sealed) February 1, 2015, letter to the Court, makes it clear that the government had not made the connection between former SA Force and DeathFromAbove until the defense sought to introduce DX E. *See also* Government's Memo of Law, at 24 n. 10.

Nevertheless, at trial the government used the grand jury investigation of former SA Force as a sword to preclude far more than the mere fact that former SA Force was under investigation, and instead employed that excuse to eviscerate the defense and its attempts to introduce evidence not covered by the Court's pretrial rulings. In addition to the DeathFromAbove, the contents of Defense Exhibit E did not reveal that former SA Force was the subject of an ongoing grand jury investigation, yet the bulk of the information therein, as well as the document itself was precluded even though, as discussed **ante**, at 4, *it was included as a Government Exhibit in the initial list provided two days after the government disclosed to the defense the grand jury investigation of former SA Force*.

The government's account, in its Memo of Law, at 13-14, of its objections to the defense's attempt to introduce the private messages from "Death From Above" demonstrates the government's true objectives in precluding the information and evidence regarding former SA's Force and Bridges, which was simply to deprive Mr. Ulbricht of a defense at trial.

Conclusion

Accordingly, for all the reasons set forth above, and in Mr. Ulbricht's prior submissions, 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: 16 April 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