



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

January 19, 2015

By ECF

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 respectfully submits this letter brief to address the admissibility of testimony the defense elicited on Thursday and seeks to continue eliciting from Special Agent ("SA") Jared Der-Yeghiayan concerning Mark Karpeles, formerly the owner of the Bitcoin exchange known as "MtGox," whom the defense apparently seeks to argue was the true operator of Silk Road. As set forth below, this line of questioning is impermissible on several grounds.

First, the line of questioning is improper insofar as it is focused on SA Der-Yeghiayan's state of mind during his investigation. That is, the defense seeks to have SA Der-Yeghiayan explain why he *believed* during an earlier period in time that there was reason to suspect Mr. Karpeles was involved in operating Silk Road. SA Der-Yeghiayan's beliefs are not evidence. Just as SA Der-Yeghiayan could not have testified on direct examination about his current belief that the defendant is guilty of the crimes charged and the reasons why he holds that belief, he cannot now be asked to testify on cross-examination about his previous beliefs that others were implicated in the crime or the reasons for those beliefs. Indeed, an agent's beliefs often rest on hearsay, hunches, or other information that is not in itself admissible. The defense cannot circumvent the evidentiary rules prohibiting the admission of such information by having the agent testify about what he believed at various points during the investigation or why he believed it.

Second, the defense should also be precluded from inquiring into discussions between Mr. Karpeles (through his counsel) and an Assistant U.S. Attorney from the District of Maryland concerning the possibility of Mr. Karpeles proffering information he believed could help authorities in their investigation of Silk Road. SA Der-Yeghiayan was not involved in and has no first-hand knowledge of those discussions; and the residual hearsay exception, which is meant to apply only in exceptional circumstances, does not provide a basis for SA Der-Yeghiayan to

testify about them. The statements the defense seeks to elicit from SA Der-Yeghiayan on this issue do not bear circumstantial guarantees of trustworthiness, nor would admitting them serve the interests of justice. Indeed, the defense seeks to use these statements for an improper purpose – to falsely suggest to the jury that Mr. Karpeles had inside knowledge about Silk Road, or sought to obtain immunity from prosecution for involvement in Silk Road, when neither suggestion is true.

Finally, to the extent the defense seeks to elicit testimony from SA Der-Yeghiayan concerning Mr. Karpeles that does not either consist of agent belief or inadmissible hearsay, the Court should allow such testimony only if the defense can show it is more probative than prejudicial. The Second Circuit has made clear that courts have an important gatekeeping role where a defendant seeks to introduce evidence of an “alternative perpetrator,” as such evidence poses serious risks of confusing and misleading the jury. In keeping with that gatekeeping role, courts allow such evidence only if the defense can proffer a substantial, direct connection – as opposed to a mere basis for suspicion – linking the “alternative perpetrator” to the crime charged. As explained below, the connections the defense seeks to draw between Mr. Karpeles and the Silk Road website are, based on what the Government ultimately learned through its investigation, neither direct nor substantial. Accordingly, the Court should carefully evaluate the probative value of any evidence the defense seeks to introduce concerning Mr. Karpeles and exclude such evidence if its probative value is outweighed by its potential prejudicial effect.

Factual Background

A. SA Der-Yeghiayan’s Investigation of Mark Karpeles

As SA Der-Yeghiayan testified during direct examination, his investigation of Silk Road spanned approximately two years. During that time, before certain information about the defendant was brought to his attention by IRS Special Agent Gary Alford on or about September 10, 2013, SA Der-Yeghiayan looked into several other individuals whom he thought potentially were involved in operating Silk Road.

One of the individuals SA Der-Yeghiayan considered was Mark Karpeles. Mr. Karpeles was, at the time in question, the owner of a company based in Japan known as “MtGox” – one of the largest Bitcoin exchanges then in operation on the Internet. SA Der-Yeghiayan’s suspicion of Mr. Karpeles was based primarily on the fact that, from February 2011 to February 2012, the website “silkroadmarket.org” was hosted on a server controlled by Mr. Karpeles. The “silkroadmarket.org” website was a simple website on the ordinary Internet that provided instructions on how to get to the real Silk Road on Tor. (*See Ex. A.*) SA Der-Yeghiayan looked up the “silkroadmarket.org” website on “who.is” (a public database discussed during SA Der-Yeghiayan’s testimony on direct), which revealed that the website resolved to a server controlled by a certain company that SA Der-Yeghiayan traced to Mr. Karpeles.

Two other considerations led SA Der-Yeghiayan to suspect that Mr. Karpeles might be involved in Silk Road. First, SA Der-Yeghiayan believed Mr. Karpeles had a motive for operating Silk Road – to generate a demand for Bitcoins (which were needed to make purchases on Silk Road), which would in turn drive customers to MtGox. Second, SA Der-Yeghiayan

noticed that certain websites he believed to be associated with Mr. Karpeles were created with certain software that was also used to create certain portions of the Silk Road website. Based on this evidence, in mid-August 2013, SA Der-Yeghiayan obtained a search warrant for certain email accounts used by Mark Karpeles so that he could review them for any evidence corroborating his suspicions.

No such evidence was found. Instead, the evidence showed that the principal basis for having suspected Mr. Karpeles prior to obtaining the search warrant did not, in fact, establish a connection between Mr. Karpeles and Silk Road. In particular, the evidence showed that, besides operating Mt. Gox, Mr. Karpeles also ran a webhosting service known as “Kalyhost” (also known as “AutoVPS.net”), which accepted Bitcoins among other forms of payment. Like any webhosting service, such as “Amazon Web Services” or “GoDaddy.com,” Kalyhost leased server space to its customers for them to use in setting up their own websites. The “silkroadmarket.org” website belonged to a Kalyhost *customer*, as evidenced, for example, by an email from the customer found in the email account for Mr. Karpeles’ webhosting company, seeking assistance with a customer-support question. (*See Ex. B*).¹

The Kalyhost customer associated with the “silkroadmarket.org” website, the investigation ultimately revealed, was the *defendant*. As reflected in the “who.is” information for the “silkroadmarket.org” website, the name of the website was registered by someone using the name “Richard Page.” (*See Ex. C*). Based on an examination of the defendant’s laptop subsequent to his arrest, that name is known to be an alias used by the defendant. Specifically, a file recovered from the defendant’s computer, within a folder marked “aliases” [sic], reflects the name “Richard Page,” along with a false address included in the contact information used to register the “silkroadmarket.org” domain name. (*See Ex. D*). The file further reflects that the information was used to rent a server from “kalyhost.” (*Id.*).

The fact that the defendant used Mr. Karpeles’ webhosting service to host the “silkroadmarket.org” website turned out to be the *only* connection SA Der-Yeghiayan ever found between the website and Mr. Karpeles. And the results of the search warrant effectively eliminated the significance of that connection. There was no evidence that Mr. Karpeles himself created or maintained the “silkroadmarket.org” website. Again, Mr. Karpeles controlled numerous servers, which he leased to a multitude of different customers who used Kalyhost as their webhosting provider; thus, the fact that the “silkroadmarket.org” website was hosted on a server Mr. Karpeles controlled does not imply he was responsible for its content.² And of course SA Der-Yeghiayan never found that Mr. Karpeles had any connection whatsoever to the servers operating the actual Silk Road website on Tor.

¹ That the operator of “silkroadmarket.org” chose to use Kalyhost to host the website is not surprising. The fact that Kalyhost accepted Bitcoins as payment made it an attractive webhosting provider for customers who wished to set up a website without having to provide identifying information in making payment.

² SA Der-Yeghiayan indicated as much during cross-examination. *See Tr.* 492:14-16 (“Q:… He [Mr. Karpeles] had a lot of domain names and things like that within his control? A: He *hosted* a lot of websites, yes.”) (emphasis added).

Once the search warrant results were obtained, and it became clear that the principal basis for SA Der-Yeghiayan's suspicion – namely, the connection between Mr. Karpeles's webhosting service and the "silkroadmarket.org" website – lacked significance, the import of the other bases for SA Der-Yeghiayan's suspicions likewise appeared insignificant. Standing alone, those other bases do not substantially implicate Mr. Karpeles in operating Silk Road. First, although SA Der-Yeghiayan suspected Mr. Karpeles of having a motive to operate Silk Road because Mr. Karpeles ran one of the largest Bitcoin exchanges in operation at the time, any operator of a Bitcoin exchange would have had a similar theoretical motive for operating Silk Road, and of course the motive for operating Silk Road was not limited to those operating Bitcoin exchanges. Second, as for the software commonalities observed by SA Der-Yeghiayan, the software in question was publicly available and widely used. Thus, SA Der-Yeghiayan had noted that a website registered to Mr. Karpeles had a "wiki" page on it (*i.e.*, an FAQ page) that was created using the same version of "wiki" software – "Mediawiki" – used to create the "wiki" page on the Silk Road website. However, Mediawiki is free, publicly available software that anyone can download.³ Similarly, SA Der-Yeghiayan also noticed that a discussion forum known as "bitcointalk.org" – which SA Der-Yeghiayan believed, based on information from a "confidential informant," was operated by Mr. Karpeles – was created using the same discussion forum software, known as "Simple Machines," used to create the Silk Road discussion forum. However, again, "Simple Machines" is publicly available software that can be downloaded for free on the Internet.⁴ (Moreover, SA Der-Yeghiayan did not develop any direct evidence that Mr. Karpeles in fact operated the "bitcointalk.org" website.) Thus, at most, this evidence shows that Mr. Karpeles used two pieces of widely available software that also happened to be used to create portions of the Silk Road website.

In short, the evidence obtained pursuant to the search warrant for Mr. Karpeles's emails, as well as the Government's investigation of the defendant, revealed no evidence that Mr. Karpeles had anything to do with operating the Silk Road website.

B. USAO-Baltimore's Efforts to Interview Mr. Karpeles in July 2013

Separately from SA Der-Yeghiayan's investigation of Mr. Karpeles, in May 2013, an agent with the Baltimore office of Homeland Security Investigations obtained a warrant to seize certain U.S.-based financial accounts associated with Mr. Karpeles' Bitcoin exchange company, MtGox, as was widely reported in the press at the time. The seizure warrant was issued pursuant to an affidavit alleging that MtGox was a money transmitting business doing business within the United States, and that Mr. Karpeles had failed to properly register the company as such with federal authorities, in violation of Title 18, United States Code, Section 1960. The same agent was also involved in an investigation of Silk Road being conducted by the U.S. Attorney's Office for the District of Maryland ("USAO-Baltimore").

SA Der-Yeghiayan learned from others involved in USAO-Baltimore's Silk Road investigation that, following the seizure of the MtGox accounts, they were seeking to interview Mr. Karpeles to determine whether he had any information concerning the operator of Silk Road.

³ See <https://www.mediawiki.org>.

⁴ See <http://www.simplemachines.org>.

(According to what SA Der-Yeghiayan had been told, the investigators did not suspect Mr. Karpeles himself of operating Silk Road, but sought any tips he might have as the operator of a large Bitcoin exchange, through which Silk Road proceeds could have passed.) In particular, according to a memo prepared by SA Der-Yeghiayan, SA Der-Yeghiayan was told in July 2013 by an AUSA in USAO-Baltimore (“AUSA-1”), that another AUSA from his office (“AUSA-2”) had spoken with an attorney for Mr. Karpeles, who had told AUSA-2 that his client was willing to provide information concerning someone whom he suspected might be operating Silk Road, in exchange for immunity from any potential charges being pursued against Mr. Karpeles for operating an unlicensed money transmitting business. SA Der-Yeghiayan subsequently learned from AUSA-1 that AUSA-2 was attempting to set up a meeting in Guam with Mr. Karpeles (who resides in Japan).

However, the meeting never materialized. SA Der-Yeghiayan was never told what specific information Mr. Karpeles had available to provide concerning Silk Road or what the provenance of it was.

C. Information Provided to USAO-SDNY by Mr. Karpeles Following Ulbricht’s Arrest

Several days after the defendant’s arrest on October 1, 2013, which was publicly disclosed the following day, the U.S. Attorney’s Office for the Southern District of New York (“USAO-SDNY”) was contacted by Mr. Karpeles’ attorney. The attorney offered to forward records associated with a certain suspicious MtGox account that he stated he had previously sent to AUSA-2 in USAO-Baltimore. The attorney stated that MtGox had also found a different account, in the defendant’s own name, which the attorney said he could supply records for as well.

Mr. Karpeles’ attorney subsequently forwarded via email the information he had previously sent to AUSA-2 concerning the account MtGox deemed suspicious. (*See* Ex. E). As reflected in the email, the attorney explained that the forwarded information was “not information about the account in Ulbricht’s name, which MtGox only identified as of interest after the Ulbricht indictment [*i.e.*, arrest].” (*Id.* (emphasis in original)). The forwarded information related instead to a MtGox account as to which “MtGox ha[d] suspicions may be associated with the largest bitcoin wallet that is perceived by some in the bitcoin community to be associated with Silk Road.” (*Id.*) (Bitcoin users had long speculated about Bitcoin “wallets” or “addresses” connected to the Silk Road website, based on analyses of the Blockchain.⁵ Thus, it appeared the MtGox account in question had transactions involving these addresses.)

The email from Mr. Karpeles’ attorney further explained that there was other suspicious activity connected to the account. The account was initially opened by someone using the email address “davidmaisano@inbox.com,” but later, when the customer was required to validate his

⁵ *See, e.g.*, Forbes Magazine, *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*, Sep. 5, 2013, available at <http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market> (discussing research paper identifying hundreds of thousands of Bitcoin addresses determined by the author to be linked to Silk Road).

identity, he did so using documents that reflected a different name from the one on the email account. Moreover, the user deposited a large number of bitcoins into the account, which he converted to nearly \$2 million in U.S. dollars, but the user never withdrew the funds off of MtGox's system to an external bank account. Eventually, the money was converted back to Bitcoins and transferred out of MtGox. However, after the transfer, the user contacted MtGox saying that he could not access the account, claiming it had been "hacked." After MtGox told the user that it appeared his credentials had previously been changed pursuant to a valid user request, the customer did not inquire further or, as far as MtGox was aware, report the hack to law enforcement, despite the large amount of funds removed from the account.

After receiving the records for the account, investigators working with USAO-SDNY's investigation of Silk Road were able to tie the "davidmasiano@inbox.com" MtGox account to the defendant through various means. For example, MtGox records showed the account being consistently accessed through IP addresses that traced back to the defendant. Moreover, transactional records from the account were included as attachments to certain emails recovered from the defendant's Gmail account, which was searched pursuant to a search warrant.

Discussion

A. The Defense Should Be Precluded from Questioning SA Der-Yeghiayan About His Past Beliefs Concerning Mark Karpeles, Which Are Not Themselves Evidence

As the defense has now made clear, the defense seeks to elicit certain testimony from SA Der-Yeghiayan in an attempt to argue that Mark Karpeles was the true operator of the Silk Road website. However, the defense's questioning thus far has focused almost exclusively on SA Der-Yeghiayan's past *beliefs* concerning Mr. Karpeles, rather than any actual facts as to which SA Der-Yeghiayan has first-hand knowledge. For example, the defense has sought to elicit, or has indicated an intention to elicit, testimony from SA Der-Yeghiayan that: (1) he at one time *believed* Mr. Karpeles was involved in operating Silk Road; (2) he at one time *believed* there was probable cause to obtain a search warrant on Mr. Karpeles' email account; and (3) he at one time *believed* that a description of the "Dread Pirate Roberts" in a Forbes Magazine article "sound[ed]" like Mr. Karpeles. None of this testimony is competent evidence. To the extent such testimony has been elicited already, it should be stricken from the record, and the defense should be precluded from pursuing similar lines of questioning going forward.

As the Second Circuit has repeatedly made clear, "[t]he agent's state of mind as the investigation progressed is ordinarily of little or no relevance to the question of the defendant's guilt." *United States v. Johnson*, 529 F.3d 493, 501 (2d Cir. 2008); *Ryan v. Miller*, 303 F.3d 231, 252-53 (2d Cir. 2002); *United States v. Reyes*, 18 F.3d 65, 70-72 (2d Cir. 1994). For this very reason, the Government cannot prove *its* case by having the investigating agent "testify to his belief that the defendant is guilty," or explain the "story of the investigation and how it progressed from suspicion to certitude." *Johnson*, 529 F.3d at 499, 501. Nor is such testimony rendered permissible if the agent attempts to explain the basis for his belief in the defendant's guilt, by summarizing, even at a general level, what led him to his conclusion. Indeed, the Second Circuit has emphasized that it only makes matters worse for an agent to give, for example, the "imprecise assurance that his belief is based on 'information from other people,

actual physical evidence, and verification through interviewing the people who are involved.” *Id.* at 499 (internal quotation marks omitted); *see also United States v. Garcia*, 413 F.3d 201, 211 (2d Cir. 2005) (finding it was “error to allow law enforcement witnesses to express opinions as to the defendant’s culpability based on the totality of information gathered in the course of their investigations”); *United States v. Dukagjini*, 326 F.3d 45, 54 (2d Cir. 2003) (expressing concerns about case agents offering “sweeping conclusions about [the defendant’s] activities”).

The same principles apply equally to the defense. Just as the Government cannot prove its case by eliciting testimony from an agent that he believes the defendant to be guilty, the defense cannot prove its case by eliciting testimony from an agent that he at one time believed someone else was involved in the crime. An agent’s beliefs about the evidence, whether favorable or unfavorable to the defendant, are simply irrelevant to what the evidence actually *is*. Moreover, an agent’s beliefs about the evidence are typically the product of various sources of information, many of which may not constitute admissible evidence by themselves. Thus, allowing testimony concerning those beliefs has the effect of introducing conclusions that rest on inadmissible foundations. As one court has put it, in commenting on the impropriety of the defense cross-examining an agent concerning his decision to close the investigation of the defendant at one point due to lack of evidence:

Whether the evidence is adequate is solely an issue for the jury, and the agent does not have any expertise, any more than anyone off the street, that would render his personal beliefs about such evidence helpful to the jury. An agent’s belief about whether the evidence was sufficient a year or two before the defendant was indicted, when the agent decided to close the case, would be even more irrelevant, if something that is irrelevant can be more irrelevant. Moreover, delving into an agent’s thoughts about the adequacy of the evidence is fraught with landmines. Not only does it involve delving into such soft evidence as the subjective thoughts of the agent, it also opens up the possibility of the introduction of such unreliable evidence as unsubstantiated leads and hearsay, which are the mainstay of an ongoing investigation but not the mainstay of a trial.

United States v. Carmichael, 373 F. Supp. 2d 1293, 1297 (M.D. Ala. 2005); *see also United States v. Demosthene*, 334 F. Supp. 2d 378, 380 (S.D.N.Y. 2004) (“[A]ny attempt by [the defendant] to dissect an individual law enforcement agent’s state of mind during the course of the investigation, or to belabor the details of the investigation’s chronological development, would be irrelevant to the central question of [the defendant’s] guilt or innocence, and as such, is inadmissible.”).

Similarly, here, the fact that SA Der-Yeghiayan suspected for a time that Mr. Karpeles possibly was involved in operating Silk Road is not itself evidence that Mr. Karpeles actually was involved in operating Silk Road. By the same token, SA Der-Yeghiayan’s belief at one point that there was probable cause to search certain email accounts used by Mr. Karpeles is, again, not itself evidence inculcating Mr. Karpeles (or exculpating the defendant). Indeed, a law enforcement agent, like any other witness, may not “present testimony in the form of legal conclusions.” *United States v. Articles of Banned Hazardous Substances Consisting of an Undetermined Number of Cans of Rainbow Foam Paint*, 34 F.3d 91, 96 (2d Cir. 1994); *accord Densberger v. United Techs. Corp.*, 297 F.3d 66, 74 (2d Cir. 2002); *cf. Rizzo v. Edison Inc.*, 419

F. Supp. 2d 338, 348 (W.D.N.Y. 2005) (“[T]he issue of whether or not probable cause . . . exists is a legal determination that is not properly the subject of expert opinion testimony.”)

Nor is it proper for SA Der-Yeghiayan to testify at a general level about what types of evidence he *thought* provided probable cause for a search warrant on Mr. Karpeles’ email accounts. Again, it would have been clearly impermissible for SA Der-Yeghiayan to testify on direct that he presently believes the defendant is guilty, and even more impermissible for him to have given “imprecise assurances” that this belief is based on various categories of evidence, such as evidence found on the defendant’s computer, evidence found in his apartment, statements of witnesses, and so forth. *Johnson*, 529 F.3d at 499. By the same token, it would be equally impermissible for the defense to elicit “imprecise assurances” from SA Der-Yeghiayan on cross-examination that there were various categories of evidence that he believed justified his obtaining a search warrant on Mr. Karpeles’ email account.

Indeed, such testimony would seriously prejudice the Government, by giving the false impression to the jury that there was a substantial body of evidence pointing to Mr. Karpeles as the operator of Silk Road, when, based on what was ultimately learned, there is no such substantial evidence. The primary evidence relied upon in SA Der-Yeghiayan’s search warrant application – the link between the “silkroadmarket.org” website and Mr. Karpeles – turned out to lack significance, as the website was simply hosted on a server controlled by Mr. Karpeles’ webhosting company. Moreover, some of the evidence relied upon by SA Der-Yeghiayan was hearsay, such as the information SA Der-Yeghiayan received from a “confidential informant” that Mr. Karpeles operated the “bitcointalk.org” discussion forum. The defense cannot paper over these evidentiary defects by simply having SA Der-Yeghiayan testify that his search warrant application rested on various types of evidence at a general level. Such testimony would mislead the jury about the quantity, quality, and admissibility of that evidence.

Similarly, the defense should also be precluded from questioning SA Der-Yeghiayan about an email he sent in mid-August 2013 expressing his belief that a description of the “Dread Pirate Roberts” appearing in an online magazine article “sound[ed] very much like MK [Mark Karpeles].” As an initial matter, the article itself is clearly hearsay and cannot be introduced through SA Der-Yeghiayan’s testimony. The article in question purported to be an interview of the “Dread Pirate Roberts,” and in it the reporter relayed that the “Dread Pirate Roberts” stated that he had bought out the previous owner of Silk Road after first gaining his trust by identifying a flaw in the site’s hardware that could be used to steal Bitcoins from the site. The defense, it is clear, is seeking to offer this statement for its truth. The defense seeks to establish (a) that the “Dread Pirate Roberts” *did* buy out the previous owner of Silk Road after initially identifying a Bitcoin-related flaw in the site and (b) that Mark Karpeles sounded to SA Der-Yeghiayan like someone who could fit this description. The latter proposition is irrelevant unless the defense is seeking to establish the truth of the former.

However, the statement of “Dread Pirate Roberts” reported in the article is clearly hearsay; indeed, it is double-hearsay. The statement was initially made by the “Dread Pirate Roberts,” and was then reported by a journalist. There is of course no reason to assume the reliability of the reported statement of the “Dread Pirate Roberts”; indeed, in the Government’s view, it is a self-serving statement of the defendant himself. *See United States v. Marin*, 669

F.2d 73, 84 (2d. Cir. 1982) (“When the defendant seeks to introduce his own prior statement for the truth of the matter asserted, it is hearsay, and it is not admissible.”); *Hubrecht v. Artuz*, No. 05 Civ. 5861 (RJH), 2008 WL 216315, at *15 (S.D.N.Y. Jan. 24, 2008) (“[S]elf-serving statements by a criminal defendant are routinely excluded as inadmissible hearsay.”). Moreover, the admission of the statement would be doubly improper given that it was filtered through a reporter. See *F.T.C. v. Medical Billers Network, Inc.*, 543 F. Supp. 2d 283, 305 (S.D.N.Y. 2008) (characterizing statements in online magazine article as “rank hearsay”).

But even putting the issue of hearsay aside, whether SA Der-Yeghiayan believed at one time that the description of “Dread Pirate Roberts” in the article resembled Mr. Karpeles in some manner is irrelevant. If the defendant seeks to prove that Mr. Karpeles has extensive expertise in Bitcoin such that he was qualified to identify a Bitcoin-related flaw in Silk Road’s system, then the defendant must do so through direct proof of that fact. Whether SA Der-Yeghiayan believed at a certain time, or even believes now, that Mr. Karpeles has such expertise is irrelevant and inadmissible – just as it would have been irrelevant and inadmissible for SA Der-Yeghiayan to have testified on direct that he believes the defendant has the expertise necessary to run Silk Road.

Accordingly, the defense should be precluded generally from eliciting testimony from SA Der-Yeghiayan concerning his beliefs about any evidence concerning Mr. Karpeles, or about any other subject, for that matter.

B. The Defense Should Be Precluded from Questioning SA Der-Yeghiayan Concerning Mark Karpeles’ Offer to Provide Information to Law Enforcement Authorities

For several reasons, the defendant should also be precluded from questioning SA Der-Yeghiayan concerning Mr. Karpeles’ offer to provide information to USAO-Baltimore in exchange for immunity from being prosecuted for operating an unlicensed money transmitting business.

First, such testimony would consist of multiple layers of inadmissible hearsay. It is apparent that the defendant seeks to elicit the testimony in order to prove the (false) proposition that Mr. Karpeles had inside information about Silk Road, indicating that he must have been involved in operating the site. The chain of hearsay through which the defendant seeks to introduce in support of this proposition is as follows: SA Der-Yeghiayan heard from AUSA-1, who in turn heard from AUSA-2, that AUSA-2 had spoken with Mr. Karpeles’ attorney (who impliedly had spoken with Mr. Karpeles), and that the attorney stated, on behalf of his client, that his client had information about Silk Road that he was willing to supply to law enforcement authorities in exchange for some form of immunity. The chain thus involves *quadruple* hearsay: Mr. Karpeles’ implied statement to his attorney that he was willing to talk in exchange for immunity, which his attorney communicated to AUSA-2, who communicated it in turn to AUSA-1, who communicated it in turn to SA Der-Yeghiayan.

There is no basis for this compound hearsay to be admitted into evidence. In particular, the residual hearsay exception of Rule 807 affords no basis to do so. That exception allows a statement not covered by the hearsay exceptions of Rule 803 to be admitted only if: “(1) the

statement has equivalent circumstantial guarantees of trustworthiness; (2) it is offered as evidence of a material fact; (3) it is more probative on the point for which it is offered than other evidence that the proponent can obtain through reasonable efforts; and (4) admitting it will serve the purposes of these rules and the interests of justice.” As the Second Circuit and courts within this district have repeatedly noted, the residual hearsay exception is meant to “be used very rarely, and only in exceptional circumstances.” *Parsons v. Honeywell, Inc.*, 929 F.2d 901, 907 (2d Cir. 1991) (internal quotation marks omitted); *see also, e.g., United States v. DeVillio*, 983 F.2d 1185, 1190 (2d Cir. 1993) (residual hearsay exception is “applied in the rarest of cases”); *Lakah v. UBS AG*, 996 F. Supp. 2d 250, 257 (S.D.N.Y. 2014) (same); *United States v. Mejia*, 948 F. Supp. 2d 311, 316 (S.D.N.Y. 2013) (same).

There are no “exceptional circumstances” that would make it appropriate to invoke the residual hearsay exception here. To the contrary, the quadruple-hearsay at issue – in essence, Mr. Karpeles’ statement that he was willing to exchange information about Silk Road for some form of immunity – clearly fails to meet the thresholds of Rule 807. First, the statement does not have strong circumstantial guarantees of trustworthiness; it can easily be misconstrued and taken out of context – precisely as the defendant seeks to take it out of context here. Specifically, it is not clear from the statement, as it was reported to SA Der-Yeghiayan, what type of information Mr. Karpeles had available to provide, or where he got it from. In fact, Mr. Karpeles merely had information about a suspicious MtGox account tied to Bitcoin addresses that some believed were associated with Silk Road; and he was merely seeking immunity from being prosecuted for operating an unlicensed money transmitting business in the wake of the seizure of MtGox’s U.S.-based financial accounts two months earlier. Thus, were the defense to elicit from SA Der-Yeghiayan his vague, fourth-hand understanding of the statement – that Mr. Karpeles was willing to provide information about Silk Road in exchange for immunity – the jury would be left with a highly misleading impression that the defense is clearly seeking to foster: that Mr. Karpeles had information about Silk Road as an *insider* and was seeking immunity from being prosecuted for involvement in operating the site.

Second, the quadruple-hearsay at issue is not evidence of a material fact. The fact that Mr. Karpeles was willing to provide information to authorities concerning Silk Road is not evidence that he was involved in operating Silk Road, as the true circumstances of Mr. Karpeles’ offer (which may not have been known to SA Der-Yeghiayan) make clear. Likewise, the fact that Mr. Karpeles sought immunity of some kind is not evidence that he was involved in operating Silk Road. Again, the immunity he sought concerned potential prosecution for operating an unlicensed money transmitting business, not prosecution for operating Silk Road.

Third, admitting hearsay testimony concerning Mr. Karpeles’ offer to talk to authorities would not serve “the interests of justice.” It is abundantly clear that the defendant’s objective in eliciting this testimony is to falsely implicate Mr. Karpeles in the operation of Silk Road. Were the Court to allow this hearsay testimony, the Government would be unable to fully correct this misimpression on redirect, given the limitations of SA Der-Yeghiayan’s knowledge about the issue. SA Der-Yeghiayan was not involved, for example, in the exchanges between USAO-SDNY and the attorney for Mr. Karpeles, in which the attorney made clear that the information Mr. Karpeles had to offer came simply from his operation of MtGox, as opposed to any involvement in Silk Road. Hence the Government cannot elicit the facts known from these

exchanges through SA Der-Yeghiayan. The hearsay rule exists to prevent precisely this sort of situation: the elicitation of a statement from a witness who heard it indirectly from others and who therefore is not in a position to testify about the underlying context in which it was made.

In short, the residual hearsay exception, which is intended to be very narrow in scope, affords no basis to allow SA Der-Yeghiayan to testify about discussions in which he was not involved, and had limited, fourth-hand knowledge, concerning Mr. Karpeles' apparent willingness to provide information to law enforcement authorities in connection with Silk Road.

C. Any Evidence the Defense Seeks to Elicit Concerning Mark Karpeles Should Be Carefully Scrutinized Under Rule 403

To the extent the defense seeks to elicit any testimony from SA Der-Yeghiayan concerning Mr. Karpeles other than agent belief or hearsay – which has been the bulk of the elicited testimony so far – the Court still must ensure that the probative value of the testimony is sufficient to outweigh any potential prejudicial effect. 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.”).

Accordingly, where evidence sought to be introduced by the defendant fails to establish a direct, substantial connection between the alleged third-party perpetrator and the crime charged, the evidence should be excluded under Rule 403. In *Wade*, for example, the defendant sought to introduce evidence that the victim of the charged murder in the case was a member of a gang who had previously participated in a shoot-out with a third-party – who the defendant alleged was the real murderer. 333 F.3d at 54-55. Notwithstanding that this evidence established a motive for the third-party to have committed the crime, and even possibly the opportunity to do so, the Second Circuit held that the evidence was properly excluded, because no evidence specifically linked the third-party to the murder. *Id.* at 60-61. Allowing the evidence, the Second Circuit found, would have “invite[d] testimony that was both distracting and inflammatory” and “posed a danger of turning attention away from issues of [defendant’s] culpability.” *Id.* at 61; *see also United States v. Diaz*, 176 F.3d 52, 82 (2d Cir. 1999) (finding that claim that murder victim had assaulted inmate while in jail, which suggested motive on the part of a third party, “was creative conjecturing and the court properly exercised its discretion in excluding such speculative evidence”).

Likewise, in a different Second Circuit case (also involving a party named Wade), the Second Circuit upheld the exclusion of “alternative perpetrator” evidence that the defendant sought to elicit during cross-examination of a police officer testifying for the prosecution. *United States v. Wade*, 512 Fed. Appx. 11 (2d Cir. 2013). Specifically, the defendant sought to elicit testimony from the police officer concerning the arrest of a third-party who had been caught dealing drugs in the same apartment building where the defendant’s girlfriend lived – in whose apartment drugs alleged to have been the defendant’s were seized. *Id.* at 14. Although the defendant argued that the arrest of the third-party established the possibility that the drugs seized in the defendant’s girlfriend’s apartment belonged to the third-party rather than the defendant, the Second Circuit found that the arrest of the third-party was not sufficiently linked to the seizure of drugs from the girlfriend’s apartment to make the theory plausible, and that allowing the police officer to testify concerning the arrest therefore “presented a risk of juror confusion and extended litigation of a collateral matter.” *Id.* (citing *United States v. Aboumoussallem*, 726 F.2d 906, 912 (2d Cir. 1984) (upholding exclusion of defense-proffered testimony to avoid a “trial within a trial”)).

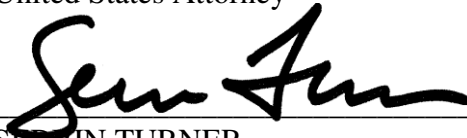
For similar reasons, the Court should carefully scrutinize any “alternative perpetrator” evidence the defense seeks to introduce in this case through SA Der-Yeghiayan. As explained, although SA Der-Yeghiayan at one time believed that Mr. Karpeles may have been involved in Silk Road, the connections he drew between Mr. Karpeles and Silk Road evaporated in the light of subsequent investigative discoveries. In order to introduce evidence that Mr. Karpeles was the “alternative perpetrator” in this case, the defense must offer evidence of a direct and substantial connection between Mr. Karpeles and Silk Road based on *actual fact* – rather than on the incomplete impression of the evidence SA Der-Yeghiayan had at a past point in the investigation. As the record currently stands, the defense has failed to offer a *bona fide* connection between Mr. Karpeles and Silk Road. Absent a competent proffer of such a connection, the Court should exclude such “alternative perpetrator” evidence, as it threatens to “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.

Conclusion

For the reasons above, the Government respectfully requests that the Court: (1) strike any testimony elicited from SA Der-Yeghiayan concerning his beliefs about Mark Karpeles and preclude the defense from pursuing such questioning further; (2) preclude the defense from questioning SA Der-Yeghiayan concerning his understanding of Mr. Karpeles' offer to provide information concerning Silk Road to law enforcement authorities; and (3) carefully evaluate under Rule 403 any evidence the defense seeks to offer concerning Mr. Karpeles other than agent belief and hearsay.

Respectfully,

PREET BHARARA
United States Attorney

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

cc: Joshua Dratel, Esq.



Silk Road

anonymous marketplace

This is not the Silk Road, but you are close...

The Silk Road is an anonymous online market. Current offerings include Marijuana, Hash, Shrooms, LSD, Ecstasy, DMT, Mescaline, and more. The site uses the **Tor anonymity network**, which anonymizes all traffic to and from the site, so no one can find out who you are or who runs Silk Road. For money, we use **Bitcoin**, an anonymous digital currency.

Accessing the site is easy:

1. Download and install the **Tor browser bundle** ([Click here](#) for instructions and non-windows users)
2. Open your new Tor browser
3. Go to: <http://ianxz6zefk72ulzz.onion>

Once inside, you will find a homepage that looks something like this:



* it takes about a minute for you to make the initial anonymous connection to the site, but afterward you should be able to browse more quickly.

So what are you waiting for? Get Tor and get to Silk Road! We'll see you inside :)

-Silk Road staff

Subject: memory upgrade
From: <staff@silkroadmarket.org>
Date: 3/18/2011 4:47 AM
To: <support@autovps.net>

how do I upgrade my memory for my VPS with autovps?

silkroadmarket.org

72.52.4.119 Record information last updated 18 hours ago

★ Save Domain To Dashboard

Hide Domain Buying Options for silkroadmarket.org

Premium	Available	Unavailable	Unavailable	Available	Available	Unavailable	Available
com \$3587.00 <input checked="" type="checkbox"/> Available	co \$12.99 <input type="checkbox"/> Available	net \$49.95 <input type="checkbox"/> Backorder	org \$49.95 <input checked="" type="checkbox"/> Backorder	info \$11.00 <input type="checkbox"/> Available	us \$10.99 <input type="checkbox"/> Available	biz \$29.95 <input type="checkbox"/> Backorder	mobi \$10.99 <input type="checkbox"/> Available

[Purchase Domains](#) [Domain Suggestions](#) [Premium Domains](#) Powered by name.com



Transfer any COM/NET domain name to Name.com for \$8.25 [Transfer Now](#)

Whois Website Info History DNS Records Diagnostics

Domain History Info for silkroadmarket.org

Want this archived information removed?

● Old Registrar Info March 12, 2011

Name	1API GmbH (R1724-LROR)
Status	CLIENT TRANSFER PROHIBITED, TRANSFER PROHIBITED

● Important Dates

Expires On	February 28, 2012
Registered On	February 28, 2011
Updated On	February 28, 2011

● Name Servers

ns1.xta.net	118.27.1.17
ns2.xta.net	178.63.62.51

● Registrar Info January 15, 2015

Name	Webagentur.at Internet Services GmbH d/b/a domainname.at (R1304-LROR)
Status	OK

● Important Dates

Expires On	May 18, 2015
Registered On	May 18, 2012
Updated On	May 18, 2014

● Name Servers

ns1.sedoparking.com	209.200.164.69
ns2.sedoparking.com	209.200.165.74

● Old Raw Registrar Data March 12, 2011

Registrant Contact Information:
 Name: Richard Page
 Address 1: 11640 Gary St
 City: Garden Grove
 State: CA
 Zip: 92840
 Country: US
 Phone: +1.7146207320
 Email: richardpage@gawab.com

Administrative Contact Information:
 Name: Richard Page
 Address 1: 11640 Gary St
 City: Garden Grove
 State: CA
 Zip: 92840
 Country: US
 Phone: +1.7146207320
 Email: richardpage@gawab.com

Technical Contact Information:
 Name: Richard Page
 Address 1: 11640 Gary St
 City: Garden Grove
 State: CA
 Zip: 92840
 Country: US
 Phone: +1.7146207320
 Email: richardpage@gawab.com

Information Updated: Thu, 15 Jan 2015 19:51:01 UTC

● Raw Registrar Data January 15, 2015

Registrant Contact Information:
 Name: Qin Shu Tong
 City: Guangzhou
 Zip: 510623
 Country: CN
 Phone: +86.7713898523
 Email: qtong77@gmail.com

Administrative Contact Information:
 Name: Qin Shu Tong
 City: Guangzhou
 Zip: 510623
 Country: CN
 Phone: +86.7713898523
 Email: qtong77@gmail.com

Technical Contact Information:
 Name: Qin Shu Tong
 City: Guangzhou
 Zip: 510623
 Country: CN
 Phone: +86.7713898523
 Email: qtong77@gmail.com

Information Updated: Thu, 15 Jan 2015 19:51:01 UTC

Evidence Tree

- pulse
- apps
- .vnc
- thumbnails
- fontconfig
- .macromedia
- gphoto
- dropbox
- pki
- samsung-tools
- freemind
- shotwell
- Pictures
- bitcoin
- Documents
 - books
 - archive
 - archive
 - 3ds
 - club-z
 - Eden
 - NYL
 - Documents
 - acton material
 - Adobe
 - Downloads
 - economics
 - EVE
 - capture
 - logs
 - Fax
 - job search
 - mind maps
 - op prof sek
 - mdma
 - misc
 - rhodium
 - security
 - aliases
 - Max Borders
 - Richard Page
 - silkroad
 - arto
 - nightcap site
 - pgp keys
 - tor
 - reference
 - Scanned Documents
 - thesis
 - to read

File List

Name	Size	Type	Date Modified
richardpage.asc	6 KB	Regular File	9/29/2009 5:49:56 AM
info.txt	1 KB	Regular File	3/20/2011 6:09:06 PM

```

Name: Richard Page
DOB: 5/13/1977
Married
addr: 11640 Gary St, Garden Grove, CA 92840, United States
phone: 714-620-7320

pgp passphrase: ██████████

richardpage@egypt.cc
██████████

kalyhost
richardpage
██████████

autoVPS
silkroad
██████████

operation fabulous
silkroad
██████████

KH mail
staff@silkroad.org
██████████

gawab:
user: mollyjane
pass: ██████████
  
```

Properties

General

Name: info.txt
 File Class: Regular File
 File Size: 375
 Physical Size: 4,096
 Start Cluster: 15,297,732
 Date Accessed: 10/2/2013 1:43:38 AM
 Date Created: 5/8/2012 8:45:09 PM
 Date Modified: 3/20/2011 6:09:06 PM
 Actual File: True

UNIX Security Attributes

Unix Permissions: -rw-r--r--
 UID: 1,000
 GID: 1,000

Ext2/3/4 Information

Inode Number: 3,802,551
 Inode Change Time: 7/12/2013 4:38:09 AM

Turner, Serrin (USANYS)

From: ██████████, Scott H <██████████>
Sent: Tuesday, October 15, 2013 11:42 AM
To: Turner, Serrin (USANYS)
Subject: FW: MtGox – F.R.C.P. Rule 11(f) / F.R.E. 410 Communication - Bradley Information
Attachments: Bradley - customer service dialogue.pdf; Bradley account verification materials.pdf

Serrin,

As discussed, I am forwarding you the materials I provided to ██████████ regarding an account that may have been related to a bitcoin wallet of interest to the government. This is not information about the account in Ulbricht's name, which MtGox only identified as of interest after the Ulbricht indictment. Please see the note below.

Scott

From: ██████████, Scott H
Sent: Wednesday, July 24, 2013 9:11 PM
To: ██████████@usdoj.gov
Subject: MtGox – F.R.C.P. Rule 11(f) / F.R.E. 410 Communication - Bradley Information

██████████,

This e-mail responds to your request for information relating to an individual that MtGox has suspicions may be associated with the largest bitcoin wallet that is perceived by some in the bitcoin community to be associated with Silk Road. Please find attached verification materials provided by a J██████████ Bradley. The materials include copies of the following: (i) a copy the Federal Express airbill used to send the materials to MtGox; (ii) a copy of a California Identification Card; (iii) a California Secretary of State Apostille, completed by a notary in Alameda County, for the California Identification Card; (iv) a Comcast bill showing a Chico, California address for Mr. Bradley; and (v) a California Secretary of State Apostille, completed by a notary in Alameda County, for the Comcast bill.

The attached materials were provided by a user for a MtGox account that was originally opened using the e-mail address: davidmaisano@inbox.com. As we described to you during our meeting in Baltimore, it has been possible to open a MtGox account without providing verification materials. Once a user met certain usage thresholds (which, as we described, have changed over time), MtGox required users to verify their identity. The attached materials were provided to MtGox to verify the account opened using the davidmaisano@inbox.com e-mail address. As you are aware, e-mail addresses are not proof of identity, and it is not uncommon for users of the internet to have e-mail addresses that are not their actual names. Once the account was verified, MtGox regarded the account as owned and controlled by J██████████ Bradley.

The user deposited a large number of bitcoins into the account. The user used the bitcoins to purchase U.S. dollars, but the account was never linked to a bank account to make a withdrawal. The transactional records for the account are too voluminous to provide via e-mail. I'm happy to discuss a method and format to provide the records to you.

In May 2013, the user contacted MtGox to report that the account was "hacked." MtGox informed the user that the e-mail address associated with the account had been changed pursuant to a proper request to change the address. A copy of the exchange with the user regarding the hack is also attached to this e-mail. Following the exchange attached to this e-mail, the user did not communicate further with MtGox, and MtGox is not aware that the user made any report to law enforcement.

Prior to the user contacting MtGox regarding the "hack", the approximately U.S. \$1.9 million had been converted to bitcoins. The bitcoins (7393.49 BTC) were transferred to address 1AsUc3Lw1oDmwimWoGeCfBngzziS98FP5V (7393.49 BTC). MtGox is aware that some of these bitcoin were used, and the balance (6393.49 BTC) currently remain at address 1Mh58EcGSMMscgh5qE5u4BVSL9KRd8GzQK. MtGox believes 1000 BTC were sold on exchange btc-e.com.

Please let me know if you have questions.

Scott



Pursuant to requirements related to practice before the Internal Revenue Service, any tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for the purposes of (i) avoiding penalties imposed under the United States Internal Revenue Code or (ii) promoting, marketing or recommending to another person any tax-related matter.

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message. Please visit [REDACTED] for other important information concerning this message.