IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

MICHAEL SEGAL, DANIEL E. WATKINS, and NEAR NORTH INSURANCE BROKERAGE, INC.

Defendants.

No. 02 CR 0112
Judge Ruben Castillo

DEFENDANTS' MEMORANDUM IN SUPPORT OF THEIR RENEWED MOTION FOR AN EVIDENTIARY HEARING AND TO SUPPRESS ILLEGALLY SEIZED EVIDENCE

Daniel E. Reidy
Thomas P. McNulty
Jeremy P. Cole
JONES DAY
77 West Wacker Drive, Suite 3500
Chicago, Illinois 60601-1692
(312) 782-3939

Attorneys for Defendant
MICHAEL SEGAL

Dated: October 31, 2003

167

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. INTRODUCTION

Adhering to the findings in the Court's August 7, 2003 ruling on Mr. Segal's original motion, defendants Michael Segal ("Mr. Segal") and Near North Insurance Brokerage, Inc. ("Near North") renew this motion for an evidentiary hearing and to suppress evidence obtained in violation of the Fourth Amendment. Defendants seek a hearing to establish that certain cooperating witnesses were acting as government agents, and, therefore, in violation of the Fourth Amendment, when they procured substantial amounts of attorney-client privileged and confidential information that had been hacked from Mr. Segal and co-defendant Near North. Defendants seek to suppress that illegally seized evidence, and also seek to suppress evidence that another cooperating witness, the former Chief Financial Officer at Near North, obtained from Near North without a warrant while acting as a government agent.

In denying Mr. Segal's original motion without prejudice, the Court described the motion as "premature" and identified various concerns, including: 1) the nature and extent of the government's connection to the hacking activity; 2) putting cooperating witnesses "on trial" before the trial of this case; and 3) the identification of specific evidence to be suppressed. Defendants have squarely addressed each of those concerns in this renewed motion, which is now buttressed by additional discovery, produced by the government since briefing on the original motion was completed. Those additional discovery materials demonstrate further how the government knew or should have known that its witnesses were providing it with information and documents that were the fruits of an illegal search.

First, regarding the extent of the government's connection to the hacking activity, defendants have now identified additional hacked evidence in the government's possession. After the Court's August 7 ruling, the defendants received long-awaited discovery contained in the FBI's so-called "1A" files maintained for this case. Among those materials, the defendants

found additional evidence regarding Near North's premium fund trust account that a cooperating witnesses had unquestionably solicited from the hacker and later provided to the government. Although the government never drafted any written report of the interview in which the cooperating witness produced this evidence to the government (illustrative of an unfortunately all-too-common investigative practice in this case), the 1A file reflects that the government received the evidence on February 26, 2002, approximately a month after Mr. Segal's arrest and six weeks after the FBI undeniably learned that its cooperating witnesses were receiving hacked material.

Second, to address the Court's concern that an evidentiary hearing would "put the government's witnesses on trial before commencement of the criminal trial," the defendants propose a bifurcated, two-phase hearing. In phase one, defendants propose that only the FBI case agents who dealt with cooperating witnesses would testify regarding the nature and extent of the government's knowledge that its witnesses were providing it with the fruits of illegal hacking activity. Then, if the defendants sustain their initial burden, or if the Court decides that additional testimony is necessary to resolve any factual issues presented, the Court can determine whether any additional witnesses should be required to testify in phase two. Defendants further propose that the scope of the testimony in both phases be confined to: (1) the government's collection of evidence from the cooperating witnesses; (2) when and how much the government knew or should have known about the hacking activity and its cooperating witnesses' involvement in that activity; (3) what inducements, incentives, and rewards the government offered or, delivered for the cooperating witnesses information delivered from illegally obtained sources; and (4) whether the witnesses were acting as government agents in soliciting and procuring illegally seized evidence without a warrant.

Third, the defendants have addressed the Court's concern that the original motion did not identify specific evidence to be suppressed. Defendants seek to suppress evidence in the government's possession that defendants will prove was hacked, based on the current, limited record. However, because of the substantial number of undocumented interviews that the government had with cooperating witnesses while they were receiving stolen information from the hacker, defendants still cannot possibly know, without an evidentiary hearing, the full extent of hacked information that the government received from the cooperating witnesses. Defendants also seek to suppress additional evidence, unrelated to illegal hacking activity, which the defense expects to demonstrate that the government unlawfully obtained without a warrant by directing another cooperating witness, while he was employed at Near North, to seize documents from Near North and later provide those materials to the government's agents.

Admittedly, the defendants' motion involves some "connecting of dots" and circumstantial evidence regarding the government's knowledge of its witnesses' participation in hacking activity, as the defense has been forced to develop exactly what occurred in this investigation largely from materials in the government's own files. The defense does not expect to prove that cooperating witnesses walked into the FBI office, announced that they were working with a computer hacker to steal confidential and privileged communications from Near North's computer network, and that the government then encouraged its witnesses to "go ahead and give us everything you get." Constitutional violations are rarely this blatant, and the law does not require such proof. Instead, the law provides that if the government knew or had reason to know that an illegal private search was taking place, did nothing to stop it from occurring or continuing, deliberately closed their eyes to it, but all-the-while accepted the fruits and

developed leads derived from the illegal private search, then the government has violated the Fourth Amendment.

Based on the limited record available to date, that is precisely what appears to have happened in this case. Below the defendants offers specific facts demonstrating that as early as the fall of 2001 (when the cooperating witnesses began procuring the hacked information) and at various intervals thereafter, the government knew or should have known that its cooperating witnesses were involved in an illegal private search and were providing information to the government derived from the unlawful search. Indeed, on January 14, 2002, twelve days before Mr. Segal's arrest and the execution of four search warrants, an FBI agent met with the cooperating witnesses and transcribed in her notes the name of the hacker, the street intersection near where he lived, and the content of an attorney-client privileged communication between Mr. Segal and outside counsel relating to the premium fund trust account that the witnesses obtained from (in the agent's own words) an "e-mail sent by hacker." The government took no action whatsoever to stop this obvious hacking activity, and continued to receive additional hacked communications from its cooperating witnesses on at least two separate occasions later in February 2002. Indeed, despite several incidents where the government admittedly learned that its cooperating witnesses were receiving stolen information from the hacker, the government cannot point to a single contemporaneous record evidencing that it admonished its witnesses not to procure, accept, or review stolen confidential or privileged material regarding Mr. Segal or Near North.

While the government has steadfastly contended that it did not know its witnesses were actively procuring hacked information, the government cannot escape the Fourth Amendment's reach by turning a blind eye toward an illegal private search. At some point in the course of its

investigation, whether it was in the fall of 2001, or two weeks before Mr. Segal's arrest, or in the months immediately after the government's initial charges, or in any one of the dozens of undocumented exchanges between the FBI and its cooperating witnesses throughout the government's long investigation, the Fourth Amendment required the government to take its head out of the sand and do what is right when it was apparent its witnesses were delivering illegally obtained information. Because that never happened here, the defendants seek an evidentiary hearing and relief from this Court.

II. PROCEDURAL HISTORY

On June 10, 2003, Mr. Segal filed his original motion for an evidentiary hearing. On July 3, 2003, the government responded, making broad, unqualified assertions that the government knew nothing about David Cheley ("Cheley") and his hacking activity. Among other things, the government asserted:

- "[N]othing even remotely suggests that the government agents were aware of Cheley or that he was an unauthorized person on Near North's computer system, until well after Near North discovered Cheley's intrusions after the arrest of Mr. Segal." (Gov't Orig. Resp. at 10.)

- "Cheley was completely unknown to the government, and nothing caused the agents to believe that any information being provided was a result of stolen or improper access to this corporation's computer network." *Id.* at 15.

- "The fact is that Cheley was completely independent of the government and unknown to the government. There is not the slightest indication that any government agent knew of unauthorized intrusions into the Near North system, let alone an illegal hacking of the system by Cheley or anyone else." *Id.* at 17.

On July 16, 2003, the government contacted defense counsel and moved to file a corrected response brief. The government represented that it had recently uncovered a "separate set of notes," transcribed by one of the case agents eighteen months earlier in January 2002 during a conversation with "three cooperating witnesses." The first page of the notes identified

Cheley by name, identified the street intersection near where he lives, and indicated that Cheley was "sending anonymous e-mails to these three (?)." (Ex. 1.) The second page of notes transcribed the substance of a hacked, attorney-client privileged e-mail sent by Mr. Segal to outside counsel regarding Near North's premium fund trust account ("PFTA"). *Id.* In the margin, the agent wrote the words -- "one e-mail sent by hacker" -- and then drew an arrow to the above note regarding the PFTA.[1] *Id.* On July 17, 2003, the government filed a corrected response and withdrew the broad assertions bulleted above.

On August 7, 2003, the Court denied Mr. Segal's motion for an evidentiary hearing without prejudice, stating:

> The Court observes that an evidentiary hearing might be necessary in the future. At this point, however, delving into whether the government's witnesses acted as agents will in essence put the witnesses on trial before commencement of the criminal trial. While reluctant to open this Pandora's box, we nevertheless are mindful of Mr. Segal's Fourth Amendment rights. If Segal renews his motion for an evidentiary hearing and outlines specific evidence that he seeks to suppress and the legal and factual grounds upon which he relies, the Court would carefully review the motion. (Mem. Op. at 11.)

[1] In its motion to file a corrected response, the government stated that the agent who transcribed the "separate" set of notes "has no present recollection of the second page of notes." (Gov't Mot. at 1.) The Court noted this representation in its August 7 ruling. (Mem. Op. at 3, n.2.) The agent's lack of memory does not in any way absolve the government of its knowledge of the hacking activity and its witnesses' providing the government with hacked information. Moreover, the "separate" set of notes attached to the government's motion to file a corrected response were two of approximately twenty pages of notes that the FBI case agent transcribed on January 14, 2002 during her meeting with the "three cooperating witnesses (Walsh, Berry, and Gallagher)." Based on the volume of notes taken, it is apparent that the agent met with the "three cooperating witnesses" for a substantial period of time on January 14, 2002. Significantly, however, there is no 302 memorializing the information obtained in the January 14, 2002 interview, including information reflecting that David Cheley was sending emails "to these 3," or that these three witnesses disclosed to the case agent the content of an attorney-client privileged e-mail regarding Near North's PFTA which, the agent noted, was contained in an "e-mail sent by hacker."

III. FACTUAL BACKGROUND

In the interest of brevity, and because the defense has described the facts in detail in previous briefing defendants summarize the pertinent facts below.[2]

A. The Cooperating Witnesses' Connection to Cheley

- David Cheley worked at Near North from approximately 1999 to 2001, at the same time that several key government witnesses, including Matt Walsh, Dana Berry, and Tim Gallagher, were executives there.

- In August 2001, Near North terminated Cheley. Beginning three days after he was fired and continuing over the next eight months, Cheley hacked into Near North's network, in his words, "at least twice a day." (Ex. 2.) He hacked from multiple desktop computers located at Kemper, where he worked as a contractor after leaving Near North, and he also hacked from computers at his home. In a four-page handwritten confession, Cheley admitted to accessing Near North's network from Kemper. (Ex. 2.) Between March 12 and April 24 alone, Cheley recorded 14,500 "hits"[3] on the Near North network, including more than 10,000 hits from his laptop computer that Cheley used at Kemper and at home.

- During many of his intrusions, Cheley had unfettered administrative access to Near North's network, including employees' e-mail, Near North's financial and accounting systems, customer files and correspondence, and Near North's file server. With administrative access, Cheley had the ability to create, delete, and/or modify files, and he could also stay up-to-date on Near North's user password list. Indeed, shortly before Near North detected his hacking, Cheley bragged to a former colleague: "I can pretty much do anything on the [Near North] network." (Ex. 3).

- Cheley focused his hacking on issues relevant to this case. In a March 20, 2002 e-mail to a former Near North colleague, Cheley boasted about having accessed Near North's "financial records" and explicitly referred to Near North's premium fund trust account, a regulatory issue that has long been the centerpiece of the government's case against Mr. Segal. (Ex. 4.)

- Around the time that Walsh began cooperating with and volunteering information to the government in the fall of 2001, Walsh and Cheley began to communicate via e-mail and the telephone. For instance, on September 21, 2001, Cheley e-mailed Walsh at Walsh's

[2] Mr. Segal incorporates by reference his Motion for an Evidentiary Hearing and Memorandum in Support, filed on June 10, 2003, his Reply in Support of his Motion for an Evidentiary Hearing, filed on August 3, 2003, and the appendices accompanying both filings.

[3] As counsel understands it, a "hit" refers to any type of selection or "click" that Cheley made while within Near North's network. For example, while Cheley was invading Mr. Segal's e-mail in-box, a "hit" would be generated every time Cheley clicked on a particular e-mail to view the message. If Cheley then clicked the "Back" button to return to Segal's in-box, this would generate another "hit." Scrolling through a particular e-mail or copying and pasting a particular e-mail, however, does not typically generate a "hit."

Aon e-mail address, and stated, "I may have some information you might be interested in so please let me know if this is your e-mail address." (Ex. 5.) Walsh confirmed that he received the e-mail, and then made a joking reference to a technical computer program manual that Cheley and Walsh discussed while working at Near North. (Ex. 6.)

- Cheley later responded as follows: "I called Jeff [Ludwig, another government witness] a couple of weeks ago and passed some info to him and he was appreciative. I am guessing based on what I've read that you, Tim [Gallagher, another government witness], and Dana [Berry, another government witness] are not real happy with [Mr. Segal]. I am personally disgusted with what NN has done not only to me but to the former management group [including Walsh, Berry, and Gallagher]. Anyway, I don't want to go into details here as to what I have or can get and how I do it but if you're interested in knowing what Segal's plans are let me know a number to call." (Ex. 7.)

- After Walsh had provided Cheley his phone number, Cheley called Walsh's office number and they talked for thirteen minutes.[4] (Ex. 8).

- Ultimately, Walsh provided Cheley with telephone numbers for fellow government witnesses Dana Berry and Tim Gallagher. Walsh also gave Cheley the number of a fax machine that Walsh clearly identified as being located in Mr. Berry's private office at Aon. (Ex. 9.)

- Over the next six months, Cheley forwarded copious amounts of confidential, proprietary, and privileged communications to Walsh and/or Berry, often in zip files.[5] Walsh forwarded to Berry whatever hacked information that Walsh received from Cheley. Although the total number is unknown, Cheley sent more than a hundred hacked communications to Walsh and/or Berry.[6]

- Cheley used various internet e-mail aliases to transmit the hacked information, such as "Lisa Chen," "Lisa Fisher," and "Lisa Rasmussen."[7]

---

[4] Moreover, according to the case agent's field notes dated September 19, 2002, Dana Berry advised on that date that Walsh "met with [Cheley] once re [ ]." (Ex. 10). This is not a typo. The agent's field notes abruptly end without providing the subject matter of the Walsh-Cheley meeting. Moreover, the 302 memorializing the agent's conversation with Berry fails to even mention that Berry advised the agent that Cheley and Walsh had once met, never mind the subject matter of their meeting. *See* footnote 7 *infra*.

[5] A zip file uses electronic compression technology to allow a person to forward multiple electronic files or e-mails in a single file. When transmitted, a "zip file" appears as a single attachment and conceals the text of the underlying files, until, of course, the recipient opens the zip file by "clicking" on it.

[6] The known universe of e-mails hacked and sent by Cheley to the cooperating witnesses has been identified based on e-mails that Aon produced in the related civil litigation. However, these documents do not represent the entire universe of communications between Cheley and the cooperating witnesses. For starters, certain of the e-mails that Aon has produced in the civil litigation refer to other e-mails between Cheley and Walsh that were not produced. Moreover, forensic analysis of the desktop hard drives that Cheley used at Kemper reveal that Cheley sent Berry at least one e-mail at his Aon e-mail address that has yet to be produced in the civil litigation.

[7] In its August 7 written ruling, the Court indicates that "in October 2001, anonymous person(s), whom the defense asserts to be Cheley, transmitted hacked material . . ." Proof that these e-mail aliases belonged to Cheley is found on the desktop computer hard drives that Cheley used at Kemper and that the government seized in May 2002. Forensic analysis of the Kemper hard drives demonstrates that Cheley accessed the internet e-mail accounts

- In at least one instance in October 2001, Matt Walsh affirmatively solicited Cheley to "please resend" a "larger" zip file. (Ex. 13). The zip file that Cheley "resent" was titled "sample.zip" and contained approximately forty-seven printed pages worth of hacked e-mails and faxes, including several privileged communications between or among Mr. Segal and in-house or outside counsel.[8]

- Walsh and Berry were not the only government witnesses who received hacked information from Cheley. In at least two e-mails to Walsh in September 2001, Cheley admitted to having already transmitted information to Jeff Ludwig, another government witness and former Near North executive who, like Walsh and Berry, joined a competitor (not AON) immediately following his employment with Near North. Cheley advised Walsh that Ludwig "seemed to appreciate" the information that Cheley had provided to Ludwig. (Ex. 5, 7).

- Although Cheley often forwarded stolen information electronically during his intrusions, he also printed hardcopies of the hacked material and maintained files for it. For instance, Cheley once noted to a former Near North colleague: "I have a large file of NNNG stuff that would surely cause major problems for the company . . . . I'll scan this stuff in when I get some time and send it to you." (Ex. 4).[9]

In its August 7, 2003 ruling, the Court appears to question whether the government witnesses knew that it was Cheley who was sending them the hacked information. (*See* Mem. Op. at 2, n.1 ("What is not clear from the emails is whether Walsh and the others immediately

(continued...)

of Lisa Chen (squid7811@yahoo.com), Lisa Fisher (ih8sno18@hotmail.com), and Lisa Rasmussen (lisa90111@excite.com) while logged onto to the Kemper network under his user name and password. *See* Ex. 11 (screen shots forensically retrieved from the Kemper hard drives that show activity in each of the above three internet e-mail accounts).

[8] To give the Court a flavor of just how many attorney-client privileged communications that Cheley hacked and forwarded to the cooperating witnesses, and how the witnesses forwarded the hacked information among themselves, defendants submit *in camera* a collection of e-mails and attachments produced by Aon in the related civil litigation. This submission includes attorney-client privileged communications contained in the various zip files forwarded by Cheley to the government's witnesses. (Ex. 12.) To avoid any risk of waiver or possible disclosure to a third party, defendants have excluded Ex. 12 from their Appendix, and are providing it *in camera* to the Court in a separate submission. The government has already been provided with this set of e-mails, with the stolen attorney-client privileged communications redacted. Walsh, Berry, and Gallagher produced the same set of e-mails in redacted form to Mr. Segal in this case in connection with a Rule 17(c) subpoena. The pages in Ex. 12 that show Cheley e-mailing hacked information to cooperating witnesses appear at pp. 12, 24, 75, 81, 89, 94, 98, 101. In those e-mails that contain a zip file icon, the contents of the zip file immediately follow the e-mail. For example, the zip file that appears on p. 24 contained all of the faxes/e-mails found in pp. 25-72. The following individuals, whose names and/or e-mail addresses appear frequently in the stolen communications, served as either in-house or outside counsel to Near North and/or Mr. Segal: Sherri Stanton, Thomas Rakowski, David Novoselsky, and Harvey Silets. (*See, e.g.*, Ex. 12, at 13, 23, 30, 32, 37-38, 49-64, 76-77, 79-80, 90-97, 101-102.)

[9] To summarize the depth, intensity, and focused nature of Cheley's hacking, defendants attach a demonstrative exhibit attached as Ex. 14.

knew that these alias emails were in fact sent by Cheley"); *id.* at 1 ("Defense exhibits show that in October 2001, anonymous person(s), whom the defense asserts to be Cheley, transmitted hacked material . . . to [Walsh and Berry]"); *id.* at 3 ("three of the government witnesses brought these anonymous e-mails to the attention of an FBI agent in a January 14, 2002 conversation"); *id.* at 4 ("Whereas the potential government witnesses suspected that the anonymous emails were simply attempts to destroy their credibility, Segal contends that the information contained in the emails was solicited by the witnesses and passed onto the Government").

However, there can be no genuine dispute, based upon the evidence summarized above and in previous briefs, and the actual string of communications between Cheley and the government's witnesses, that the witnesses knew it was Cheley who was sending them the hacked information. For example, the communications between Cheley and Walsh in the days immediately preceding Cheley's transmission of stolen information contemplate that Cheley was getting information from an improper source. (*See, e.g.*, Ex. 7)("I don't want to go into details here as to what I have or can get and how I do it but if you're interested in knowing what Segal's plans are let me know a number to call"). Cell phone records establish that Walsh and Cheley spoke by phone for nearly fifteen minutes shortly after this e-mail. (Ex. 8.) Walsh then later carefully provided Cheley with work phone numbers for Berry and Gallagher, and made clear that Berry had a private fax machine in his private office. Moreover, Walsh was fully aware at this time that Cheley no longer worked at Near North. (*See* Ex. 5,6). In addition, Walsh's unsolicited reference to the "Zope" computer program manual in his initial e-mail response to Cheley demonstrates, at a minimum, that Walsh remembered that Cheley worked with the IT department at Near North. (*See* Ex. 6.) Given these circumstances, any argument that Berry and Walsh did not know that Cheley was the sender of the hacked information strains credulity.

In addition to questioning whether the witnesses knew that it was Cheley who was sending them hacked information, the Court also seemed reluctant in its August 7 opinion to accept the characterization of certain exchanges between Walsh and Cheley as "cover-up" e-mails. The Court's opinion quotes one of the "cover-up" e-mails that Walsh sent to Cheley, suggesting that it may have been sent in good faith: "The day after receiving the first zip file, Walsh emailed Chen the following message: 'I recognize that these were sent in error and contain information that upon first glance I did not wish to receive and you did not intend to send. Hence it has been deleted without any review.'" *Id.* at 2. The Court then notes that Cheley sent Walsh two other zip files of Near North information during October 2001. *Id.*

This e-mail suggesting that Walsh "did not wish to receive [Cheley's zip file]" and "deleted [it] without any review" is demonstrably bogus for several reasons. (Ex. 15). First, one month after Mr. Segal's arrest, Walsh provided the government with several pages of hacked e-mails that originated in the zip file that Cheley had sent him in October 2001, the very same file that Walsh falsely stated he "deleted without review." (Ex. 16). Second, neither Walsh nor the government can reasonably claim that Walsh "did not wish to receive" the information, because Walsh had explicitly asked Cheley, just two hours earlier, to "resend" the "larger" cache of hacked information. Third, the triggering event for Cheley to transmit the zip file to Walsh was an e-mail from Cheley to Walsh earlier in the day, in which Cheley expressed concern to Walsh that Cheley's true name might appear on the "file structure" of the zip file. (Ex. 17)("Did you get my e-mail on deleting the file structure of the document? I'm a little worried that there's a user name there.") Walsh, concerned about his own exposure, tried to put Cheley at ease with a formal falsely indicating that Walsh deleted the zip file without reviewing its contents response (Ex. 15)(*e.g.* "I did receive the instructions . . . , and will utilize [sic] it [sic] immediately) Hence,

it has been deleted without any review.") Not only is the tone between Walsh and Cheley inconsistent with their previous correspondence, but Walsh cleverly transformed Cheley's request to delete Cheley's name from the file structure into a "request" to "delete" all of the information sent. *Id.* Finally, just three hours before Walsh claims to have deleted the hacked information without any review, Walsh admitted to Cheley that "someone else" had been able to open the zip file for him. (Ex. 18)("someone else got it open/thanks"). Based on the record before the Court, there is no good faith argument that the above e-mail was anything but a transparent and feeble attempt to cover Walsh's and Cheley's tracks, and that Walsh reviewed the entire file and shared it with other witnesses and, at least in part, with the government. (*See* Ex. 19, 20.)

B. The Government's Exposure to the Hacking Activity

While the above facts inextricably link the government's witnesses to the hacker, there are many facts tending to show that the government knew or should have known about its witnesses' procurement of hacked information:

- The lead FBI case agent and one of the prosecutors advised counsel for Near North that they knew in the fall of 2001 that a cooperating witnesses had received "unsolicited" and "anonymous" e-mails containing confidential information about Mr. Segal and/or Near North. Walsh has similarly attested to having alerted the FBI of his receipt of purportedly "anonymous" e-mails in the fall of 2001. (Ex. 21.)

- On January 14, 2002, an FBI case agent met with the "three cooperating witnesses" and transcribed in her notes David Cheley's name, the street intersection near where he resides, and that Cheley was "sending anonymous e-mails" to the cooperating witnesses. The agent also transcribed the content of an attorney-client privileged e-mail between Mr. Segal and outside counsel regarding Near North's premium fund trust account, and indicated that the information came from an "e-mail sent by hacker." (Ex. 1.)

- On February 8, 2002, Walsh sent a hacked e-mail to the lead case agent's home e-mail address, claiming "[a]s noted in the past, from time to time I receive these anonymously." The government has not produced any record of this February 8, 2002 exchange, nor has it produced any evidence or reports reflecting that Walsh had "noted" to the government his receipt of hacked emails "in the past.".(Ex. 20).

- On March 4, 2002, Cheley sent Berry a hacked e-mail between Mr. Segal and Harvey Silets, Mr. Segal's former criminal defense counsel in this case. Berry has attested to forwarding a redacted version of the e-mail "to the FBI upon receipt." (*See* Ex. 22). Despite the obvious significance of such an event, the government has not produced any contemporaneous record of this exchange between its witness and the FBI in the spring of 2002.

- On September 19, 2002, two days after Near North's counsel met with the government to discuss the company's filing of a civil suit based on the hacking activity and the prosecutors' disavowal of any connection between Cheley and the cooperating witnesses, the lead case agent suddenly memorialized how *more than six months earlier*, Berry had received a defense camp e-mail between Mr. Segal and Mr. Silets.[10] (Ex. 23).

- The lead case agent also wrote a 302 on January 6, 2003 based on a telephonic conversation with Walsh. In this 302, the lead case agent stated that Mr. Walsh "*had previously related* that he had received unsolicited e-mails that contained what appeared to be e-mails of Michael Segal." (Ex. 24)(emphasis added). Again, the government has not produced any contemporaneous 302s or other memorialization of those instances where the witness "had previously related" that he received "unsolicited" e-mails.

In addition to these facts, defendants have identified at least one instance where the government subpoenaed a witness to testify before the Grand Jury after her name appeared in a hacked attorney-client privileged e-mail between Mr. Segal and his criminal defense counsel. In the e-mail, Mr. Segal identified a former Near North employee "with helpful information and potential specific information as to our key issues." Later, the witness, a relatively low-ranking employee in Near North's accounting department, testified before the Grand Jury. It is unclear on what date, if any, the government first interviewed this witness because defendants have not been provided with any 302 memorializing her interview. *Id.*

[10] After reading the agent's field notes from which this 302 was written, it is obvious that the agent failed to include in the 302 significant pieces of information provided by Dana Berry during this September 19, 2002 phone call. For example, the last two items in the agent's field notes read as follows: "I know the name Dave Sheley vaguely but couldn't pick them [sic] out of the line-up. Matt had met w/ him once re." (Ex. 10). While the abrupt ending of the raw field notes (without ever identifying the subject matter of Walsh's meeting with Cheley) is odd in and of itself, the fact that the agent selectively omitted information regarding a meeting between the hacker and one of the government's witnesses from his report raises concerns about the factual completeness of, and exclusion of potential *Brady* material from, this and other 302 reports maintained in this case.

C. The Abundance of Unmemorialized Contacts Between the Government and Its Cooperating Witnesses

A third area of facts critical to this motion is the vast number of unmemorialized conversations that appear to have taken place between cooperating witnesses and the government. These numerous unreported government interviews underscore the need for an evidentiary hearing, to determine exactly what the government was being told by its witnesses, and whether the government knew or should have known that its witnesses were feeding them illegally seized information. Below are just a few illustrations:

- Berry signed and submitted an affidavit in the related civil litigation, attesting that "at the time of Walsh's receipt of the first [purportedly anonymous] e-mail [from Lisa Chen], I had already been extensively interviewed by the U.S. Department of Justice regarding [Near North] and Segal." (*See* Ex. 22). The first known e-mail that Walsh received from Lisa Chen is dated October 1, 2001. While Berry has sworn that by October 1, 2001 he had already been "extensively interviewed" by the government, the first Dana Berry interview memorialized in a 302 and produced to the defense occurred on October 23, 2001.

- Tim Gallagher, like Berry and Walsh, joined Aon after leaving Near North in the summer of 2001. While Walsh was laying the groundwork with Cheley, Walsh forwarded to Gallagher at least some of Walsh's e-mail correspondence with Cheley. (*See, e.g.* Ex. 25). Between September 2001 and July 2002, Gallagher placed approximately sixty-six calls from his cell phone to the FBI main number, or to an FBI agent's cell phone number. (These sixty-six calls do not include any return or incoming calls received by Gallagher on his cell phone, or any calls that Gallagher placed to or received from the FBI at his home or office phones.) Twenty-one of these calls occurred before Mr. Segal's arrest and the execution of multiple search warrants on January 26, 2002. Mysteriously, the government's case file contains only two 302s for Gallagher, one dated January 23, 2002 and one dated July 12, 2002. The former is one sentence long and merely memorializes Gallagher's call to Mr. Segal to set up the Saturday meeting where Segal was ultimately arrested. The remaining contacts between Gallagher and the government are never memorialized in any investigative report.

- Tom McNichols is a former Near North CFO who left Near North in January 2002, less than a week before Mr. Segal's arrest. He began cooperating with the government, however, at least as early as October 18, 2001, the date of the first Source 302 attributable to him. Based on McNichols' cell phone records, he either placed or received (on his cell phone alone) approximately 225 phone calls to or from an FBI number between October 24, 2001 (the earliest date that the defense has been able to obtain cell phone call detail for McNichols) and June 18, 2002. Approximately 150 of those calls

occurred before Mr. Segal's arrest on January 26, 2002. Despite this voluminous number of calls, only a tiny fraction of Mr. McNichols' contacts with the FBI are memorialized contemporaneously in 302s.

- The same can be said for Walsh and Berry. Defendants can identify at least ten calls that Walsh placed and at least eleven calls that Berry placed to the FBI main number or the lead agent's cell phone number between February 14, 2002 and April 9, 2002 (*i.e.* during Cheley's hacking spree) that are not memorialized in a 302 or in any field notes in the confidential source files.

D. Newly-Discovered Hacked Evidence in the Government's Possession

Several weeks after the Court's August 7, 2003 ruling, the defense finally received a significant amount of additional discovery relevant to this motion. On September 18, 2003, the government produced copies of the 1A material maintained by the FBI in this case. Among these materials is additional hacked information that the government received from one of its closely-cooperating witnesses on February 26, 2002, approximately six weeks after a government case agent had noted that Cheley was sending anonymous e-mails to the cooperating witnesses. On February 26, 2002, the government received approximately twenty pages of printed e-mails from a confidential "Source" witness (believed to be Walsh).[11] (Ex. 16). The 1A envelope describes the enclosed e-mails as "Various Documents -- Primarily E-mails From Source Re: Near North Insurance - Michael Segal." *Id.* The first two pages in the 1A envelope (Bates No. 3271-72) are a printout of an August 28, 2001 e-mail from a Near North executive to Mr. Segal, describing a conversation between the executive and another Near North employee about whether the employee was going to leave Near North for a competing insurance brokerage firm. *Id.* The e-mail specifically discusses Near North's premium fund trust account.

[11] Walsh is either a recipient or author of many of the e-mails provided to the government on February 26, 2002, and therefore the defense believes that Walsh is the Source for these materials.

The content, font, and pagination of the e-mail printout found in the February 26, 2002 1A file (Bates No. 3271-72) match perfectly with the printout of a hacked e-mail that Cheley sent to Matt Walsh in a zip file on October 1, 2001, along with dozens of other confidential and/or attorney-client communications. (*Compare* Ex. 26 with Ex. 27.) The legend "notes6.txt" that appears at the top of the hacked e-mail in the FBI 1A envelope (Ex. 26) corresponds with the "notes6" legend that appears at the top of the same hacked e-mail produced by Aon in the related civil litigation. (Ex. 27). The heading and format of this email differs markedly from that of other e-mails provided to the government by Walsh that were printed from a user's screen with standard email software, and it is readily apparent from the face of the document that the text has been downloaded and "cut-and pasted" from some other source. *Id.* In addition, the government has not produced any written record (contemporaneous or otherwise) of the February 26, 2002 meeting in which Walsh provided these e-mails to the government.

While this apparently undocumented exchange of information is nothing new in this case, it once again illustrates the defendants' need for an evidentiary hearing. Without one, the defense and the Court have no way of determining, among other things, what Source (Walsh) told the government about the origin of the e-mails he was deliveries to the government whether the government solicited or rewarded its source in connection with the stolen e-mails, and whether the government knew or should have had additional reason to know that this e-mail had been hacked (falling so closely on the heels of a fellow agent's notes only weeks earlier, confirming that Walsh had received e-mail from a hacker).

IV. LEGAL FRAMEWORK FOR ANALYSIS

The Court is already familiar with the law applicable to this motion. In determining whether a private party has acted as an "instrument or agent" of the government for purposes of the Fourth Amendment, courts are to consider: 1) whether the government knew of and

acquiesced in the private party's intrusive conduct; 2) whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further his or her own ends; and 3) whether the private party acted at the request of the government or whether the government offered the private party a reward. *See United States v. Crowley*, 285 F.3d 553, 558 (7th Cir. 2002); *United States v. Shahid*, 117 F.3d 322, 325 (7th Cir. 1997); *United States v. Feffer*, 831 F.2d 734, 739 (7th Cir. 1987). Courts decide whether a private party acted as an "instrument or agent" of the government on a case-by-case basis and in light of all the circumstances. *United States v. Koenig*, 856 F.2d 843, 847 (7th Cir. 1988); *Feffer*, 831 F.2d at 739. The movant has the burden of proof and must show by a preponderance of the evidence that the private party acted as an instrument or agent of the government. *Shahid*, 117 F.3d at 325; *Feffer*, 831 F.2d at 739.

The defendants need not prove that the government explicitly asked the private party to conduct a search on its behalf, nor must a defendant present "clear" evidence that the private party acted as an agent, or even that the government acted improperly. *United States v. Stein*, 322 F. Supp. 346, 348-49 (N.D. Ill. 1971)(despite no "clear" evidence that the private party acted as the government's agent and no finding that the government acted improperly, court granted defendant's motion to suppress documents allegedly stolen by a private party who shared the defendant's office; because the government displayed "a clear pattern . . . to procure the cooperation of [the private party]," the court had "ample reason to believe that [the private party] thought the government would reward him for turning over [the] records," and the government was not "totally divorced" from the gathering of the stolen information); *Knoll Assocs., Inc. v. Federal Trade Comm.*, 397 F.2d 530, 535 (7th Cir. 1968)(where employee stole documents from his employer, and the FTC knew of the theft but nonetheless accepted and used the documents against the defendant in an FTC hearing, court found that the FTC violated the Fourth

Amendment and suppressed evidence). Nor can the government avoid the Fourth Amendment's reach by turning a blind eye to illegal private searches by cooperating witnesses. *See United States v. Mekjian*, 505 F.2d 1320, 1328 (5th Cir. 1975)("If government officials were aware, or should have been aware, that [the witness] was removing and copying records for [the government's use], [the government] will not be permitted to stand by or blink [its] eyes and accept the benefit of her activities").

Where, as here, resolution of factual issues is necessary in deciding whether evidence was obtained in violation of the Fourth Amendment, courts should conduct an evidentiary hearing. *See United States v. Sims*, 879 F. Supp. 883, 888 (N.D. Ill. 1995)(quoting *Nechy v. United States*, 665 F.2d 775, 776 (7th Cir. 1981)). The party requesting the evidentiary hearing must show that there are disputed issues of material fact necessitating a hearing. *Sims*, 879 F. Supp. at 888. As long as the factual issues presented are "definite, specific, detailed, and nonconjectural," an evidentiary hearing is justified. *Id.* (quoting *United States v. Hamm*, 786 F.2d 804, 807 (7th Cir. 1986)).

V. ARGUMENT

A. The Government Acquiesced in its Witnesses' Procurement of Hacked Information

Based on the record available to date, the government's conduct in this case epitomizes acquiescence in its cooperating witnesses' participation in an illegal private search, which in turn relied upon pervasive hacking into defendants' computer network system by Chelcy. In at least five separate instances during its investigation and prosecution of this case, starting in the fall of 2001 and continuing through March of 2002, the government either had reason to know (or was flat out told) that its closely-cooperating witnesses were receiving hacked information. Indeed, by no later than January 14, 2002, the government knew the hacker's name and knew where he

lived. Yet the government cannot point to a single piece of paper memorializing any government effort to stop the hacking activity, or any effort to admonish its cooperating witnesses not to provide it with knowingly hacked information.

A simple timeline of the key events drives this point home. Walsh has attested to having alerted the government "in the fall of 2001" that he was receiving "anonymous" e-mails containing confidential communications regarding Mr. Segal and/or Near North.[12] (Ex. 21.) *The government did nothing at this point to stop the hacking activity or its witnesses' receipt of hacked material.* On January 14, 2002, an FBI agent met with the cooperating witnesses and transcribed the contents of an attorney-client privileged e-mail between Mr. Segal and Near North's in-house counsel relating to Near North's premium fund trust account, the centerpiece of the government's case against Mr. Segal. The agent noted that the cooperating witnesses obtained the information from an "e-mail sent by hacker." The agent transcribed in her field notes Cheley's name, a street intersection near his residence, and that Cheley was "sending anonymous e-mails to these three (?)" *The government did nothing at this point to stop the hacking activity or its witnesses' receipt of hacked material.* On February 8, 2002, Walsh forwarded another hacked e-mail to the lead case agent at the agent's home e-mail address. The agent has no record of receiving this e-mail, and never made any report or other record of its receipt. *The government still did nothing to stop the hacking activity or its witnesses' receipt of hacked material.* On February 26, 2002, Walsh provided the lead case agent with a stack of printed e-mails involving Mr. Segal and/or Near North, including one that the cooperating witness had solicited and received from Cheley in a zip file. The hacked e-mail referenced Near North's premium fund trust account, the e-mail's font, pagination, and appearance were

[12] The lead case agent and one of the prosecutors have similarly admitted to receiving this information from Walsh in the fall of 2001.

substantially different from the rest of the e-mails in the stack, and the e-mail was clearly downloaded and "cut-and-pasted" from some other source. The FBI agent failed to document the conversation in which he received the stack of e-mails. *The government still did nothing to stop the hacking activity or its witnesses' receipt of hacked material.* On or around March 4, 2002, six weeks after Mr. Segal's arrest, Cheley sent Berry an attorney-client privileged e-mail between Mr. Segal and Harvey Silets, Mr. Segal's then-criminal defense counsel. Berry has attested to alerting the FBI about this and forwarding a redacted version of the email to the FBI "upon receipt." (Ex. 22.) *The government did nothing to stop the hacking activity or its witnesses' receipt of hacked material.* In fact, the FBI agent failed to memorialize this event (*i.e.* a cooperating witness's receipt of a post-arrest, ***defense camp*** e-mail) until six months later, after prosecutors had vehemently denied in a meeting with Near North's counsel any connection whatsoever between Cheley and the cooperating witnesses.

Cheley's hacking continued until April 23, 2002 when Near North (not the government) put an end to it. Were it not for Near North's own detection mechanisms, Cheley might very well still be hacking today. According to Webster's, the term "acquiesce" means "to consent or comply without protest." Webster's II New College Dictionary, at 10 (2001). Here, the government repeatedly consented to and complied with its witnesses receipt of hacked information, without the slightest sign of protest or even faint concern. The government's conduct in this case is garden-variety acquiescence in its witnesses' procurement of hacked material, and that acquiescence supports a finding that the cooperating witnesses were acting as agents of the government while receiving the fruits of illegally obtained evidence.

B. The Witnesses Procured The Hacked Information To Help The Government, Which, In Turn, Would Further Their Own Ends

The defense has presented compelling evidence that the cooperating witnesses who solicited and received hacked information did so to help the government. Before recapping that evidence, however, we first turn to a threshold issue, whether the witnesses' motivation to help the government is truly inconsistent with their desire to gain personal benefit.

In its August 7, 2003 ruling, the Court noted what it described as inconsistent arguments made by Mr. Segal about the cooperating witnesses' motivation in procuring the hacked information. The Court indicated that, in his motion for an evidentiary hearing, Mr. Segal contended that the witnesses procured the stolen information to help the government, yet, in his response to the government's motion to quash the Perkins Coie subpoena, Mr. Segal suggested that the cooperating witnesses were motivated by an improper business-related purpose. (Mem. Op. at 11.) The Court noted that any contention that the witnesses were motivated by improper business-related reasons weighs against a finding that the cooperating witnesses acted as government agents.

Mr. Segal agrees that a private party who conducts an illegal search solely for his or her personal benefit is less likely to be deemed a government agent than a private party who derives no personal benefit from conducting the search. However, it is unrealistic to treat the motivations to help the government, on one hand, and to benefit personally, on the other hand, as being mutually exclusive. This is especially true in this case, where the cooperating witnesses' pecuniary interests are tied directly to the government's investigation and prosecution of Mr. Segal. Put simply, the more the cooperating witnesses helped the government bury Segal and Near North, the more the witnesses stood to gain financially (since they had become competitors

of Near North as producers at a competing insurance brokerage). There is nothing inconsistent or contradictory about these dual motivations.

Given that the witnesses' motivation to help the government is consistent with a desire to benefit personally, Mr. Segal identified specific facts in the earlier briefing tending to show that the cooperating witnesses procured the hacked information to help the government. First and foremost, cooperating witnesses Walsh, Berry, and Gallagher no longer contest that they received stolen Near North property from Cheley. Instead, they have resorted to a tellingly brazen "defense" in the civil case that is central to this motion in many respects. At a discovery conference in the civil case last April, the cooperating witnesses' attorney, Eric Brandfonbrener, represented to the court: "We're not using these e-mails except in connection with our cooperation with the government." (Ex. 28.) Brandfonbrener further stated that "we're not using these e-mails for any purpose, and . . . these e-mails are only going to the FBI." *Id.*

In its August 7, 2003 order, the Court suggests that this statement, when read in context, "only indicates that the emails were forwarded to the FBI in order to protect the witnesses from a potential set-up by Segal and NNIB, not that they were being forwarded to substantively assist the government." The defendants respectfully disagree. While the witnesses' counsel flip-flopped throughout the civil case hearing on exactly why his client forwarded hacked material to the government, he unequivocally declared at one point that Walsh accepted hacked information and provided it to the FBI in September 2001 because he thought it "might be relevant to the government's investigation." (Ex. 28, at 71-72)("[W]hen a person named David Cheley contacted Matt Walsh in September of 2001 saying he had information regarding Near North, *Mr. Walsh agreed to accept it and Mr. Walsh told the F.B.I. about it.* This is not information that's being used for competitive purposes. This is not information that he is eliciting for

himself. *This is information he thought might be relevant to the government's investigation.*")(emphasis added).[13] Therefore, it is clear from the cooperating witnesses' own agent's statements that their participation in the hacking activity, and the provision of the fruits of the hacking to the FBI, were done primarily to assist the government in its investigation and prosecution of the defendants. *Id.*

C. The Government Has Provided the Cooperating Witnesses With Substantial Rewards

Turning to the third factor, there are numerous instances in the course of this investigation and prosecution where the government appears to have gone out of its way to protect and reward its cooperating witnesses. While the government always has a legitimate interest in protecting its key witnesses from harassment or unnecessary hardship, the treatment and rewards afforded the cooperating witnesses in this case seem extraordinary.

Again in the interest of brevity, defendants will summarize some of the rewards that the defense is aware of that the government has provided to its cooperating witnesses Walsh, Berry, and/or Gallagher[14]:

- The government has steadfastly maintained a hostile attitude toward the civil suit brought by Near North against these witnesses (before the government had initiated its prosecution of Mr. Segal), going so far as to identify the civil suit in a bill of particulars as the sole instance of purported "retaliatory litigation" alleged in the RICO count facing Mr. Segal. (*See* Segal Mem. at 22-23) The witnesses have predictably leveraged the government's characterization of the case as "retaliatory litigation" before other tribunals and in the marketplace.

- The government has provided the witnesses with advance knowledge of the government's investigation, which the witnesses, in turn, have used to persuade Near North employees and/or business partners to leave Near North in favor of

[13] The notion that Mr. Segal orchestrated Cheley's hacking activity to "set-up" or "intimidate" the cooperating witnesses is as unfounded as the cooperating witnesses' claim that the hacked e-mails were sent to them anonymously. There is not a shred of evidence to support such a theory.

[14] Defendants refer the Court to Mr. Segal's Memorandum in Support of his Motion for an Evidentiary Hearing ("Segal Mem."), filed on June 10, 2003, and his Reply in Support of his Motion for a Evidentiary Hearing ("Reply"), filed on August 1, 2003, for a more detailed explanation of these rewards.

Aon. (*See* Segal Mem. at 23.) The witnesses also aggressively spread word of Mr. Segal's arrest to the media. Indeed, on January 28, 2002, the Monday following Mr. Segal's Saturday arrest, Walsh called three different Chicago television and radio stations beginning at 6:30 a.m., and Gallagher placed six calls to the Chicago Tribune between 7:26 and 8:08 a.m. The defense understands that the government did not issue a press release regarding Mr. Segal's arrest until the afternoon of January 28, 2002.[15]

- The government appears to have provided its witnesses' private counsel an unsigned copy of the first superseding indictment, the same day that the indictment was entered on the Court's docket; the document appears to have been quickly routed to one of the witnesses, who then faxed it from his private fax machine at Aon to an unknown location. (*See* Segal Mem. at 24.)

- Despite Near North's prompt and full cooperation with law enforcement authorities, the government has not charged Cheley or others to whom he sent stolen and hacked information with any crime whatsoever, even though eighteen months have passed since Cheley confessed in writing to hacking into Near North's network "at least twice a day" over an eight-month period. (*See* Segal Mem. at 23, n.19.)

- The government has indicated to defense counsel that the government granted its key witnesses with immunity from prosecution. The defense is still waiting for the government to produce documents reflecting immunity agreements and any other benefits extended to its cooperating witnesses.

In addition to these rewards, the cozy relationship between the government and its witnesses is further demonstrated by e-mail correspondence between the cooperating witnesses' counsel (Brandfonbrener) and the government. On January 8, 2003, Brandfonbrener e-mailed the prosecutor (copying Walsh, Berry, and Gallagher), providing the government with a real-time update on discovery in the allegedly "retaliatory" civil suit. (Ex. 29.) The content and informal tone of the e-mail suggest that the government and the cooperating witnesses' counsel may have regularly provided information to each other via e-mail regarding their cases.[16]

---

[15] To provide an overview of the extensive telephone contacts between the cooperating witnesses and the government, and between the cooperating witnesses and the media, defendants attach as Ex. 30 a demonstrative exhibit reflecting certain phone calls placed by the cooperating witnesses to either the government or the media in January 2002.

[16] Pursuant to the Court's August 7, 2003 order, Brandfonbrener's law firm, Perkins Coie, should have submitted this e-mail (Ex. 29) to this Court in camera on or before August 27, 2003, along with any other documents and/or e-mails that were sent to the government relating to Near North, Mr. Segal, the cooperating witnesses, or

D. The Government Appears To Have Used Another Cooperating Witness To Unlawfully Seize Documents from Near North Without a Warrant

Mr. Segal has developed additional evidence to suggest that the government may have been using certain witnesses as its agents to unlawfully seize documents from Near North during the covert phase of the government's investigation. As noted above, Tom McNichols is a former Near North CFO who left Near North shortly before Mr. Segal's arrest. McNichols, however began cooperating with the government some time in October 2001, approximately three months before he left the company. On October 25, 2002, McNichols received multiple phone calls from the FBI early in the day, and then later that same day produced to the government a Near North document that is clearly central to the allegations of the indictment. According to a McNichols' "Source" 302, dated October 25, 2001, McNichols supplied the government that day with a document entitled "NNIB Petty Cash Reimbursement - 2001." (Ex. 31) That same day, McNichols had received three incoming phone calls from the FBI on his cell phone alone: two lasted three minutes and the third lasted four minutes. McNichols also placed a two-minute call on his cell phone to a cell phone number believed to belong to an FBI agent.

The 302 dated October 25, 2002, indicates that McNichols received the "Petty Cash Reimbursement" document from "Watkins," a co-defendant who at the time worked as an accountant at Near North, and later (sometime after October 25, 2002) became a government source and cooperating witness. Based on audiotapes produced in discovery, McNichols consensually recorded a conversation with Watkins in his Near North office in the mid-to-late afternoon of October 25, 2001 (*i.e.* shortly after the four multiple-minute conversations that McNichols had with the FBI that day), and then initiated a lengthy conversation with Watkins

(continued...)

their employer. After the government moved to quash a defense Rule 17(c) subpoena issued to Perkins Coie, the Court indicated that it would review responsive documents in camera and then decide whether these documents

about petty cash. If McNichols was acting as a government agent when he seized the "NNIB Petty Cash Reimbursement - 2001" document, as it appears he was, then the document should be suppressed. Similar to the hacking activity, an evidentiary hearing will confirm whether the government indeed used McNichols to obtain Near North documents without a warrant.

E. The Court Can Conduct a Two-Phase Hearing To Spare the Government's Witnesses from Unnecessary Cross-Examination before Trial

In its August 7, 2003 order, the Court raised concerns about "put[ting] the witnesses on trial before commencement of the criminal trial" and the lack of parameters and scope of the requested hearing. (Mem. Op. at 9, 11.) To allay these concerns, defendants propose a bifurcated hearing, in which the case agents who dealt with the cooperating witnesses would testify in phase one of the hearing. If the Court deems further evidentiary proceedings appropriate at that point, the Court could conduct a second phase where the cooperating witnesses would testify. As to the scope of the hearing, Mr. Segal proposes that phase one should be limited to the government's collection and memorialization of evidence from cooperating witnesses that is derived from hacking activity. Phase two, if necessary, should be similarly limited to the nature, content, and particulars of the witnesses' communications with the case agents regarding illegally hacked evidence, and their relationship with the hacker.

VI. CONCLUSION

Because of the abundance of apparently undocumented communications between the cooperating witnesses and the government during the time frame that the witnesses were receiving hacked information from Cheley, the defendants simply cannot identify at this time all of the evidence that they seek to suppress in connection with this motion. Nevertheless, based on

(continued...)
should be produced to the defense.

the limited record currently available the defendants seek to suppress the following evidence obtained in violation of the Fourth Amendment: 1) all evidence obtained by the FBI case agent in her January 14, 2002 meeting with the cooperating witnesses; 2) the e-mail print out (Bates No. 3271-72) obtained by the FBI from "Source" on February 26, 2002; 3) the "NNIB Petty Cash Reimbursement -2001" document identified in the Source 302 dated October 25, 2001; and 4) all leads and derivative use that the government obtained by direct or indirect use of the above evidence.

For the foregoing reasons, the defendants respectfully request that the Court: 1) suppress the evidence identified above; 2) conduct a two-phase evidentiary hearing as proposed by defendants above; and 3) fashion other remedies that it deems appropriate as a result of the evidentiary hearing.

Dated: October 31, 2003

Respectfully submitted,

Daniel E. Reidy
Thomas P. McNulty
Jeremy P. Cole
JONES DAY
77 West Wacker Drive, Suite 3500
Chicago, Illinois 60601-1692
(312) 782-3939

Attorneys for Defendant
MICHAEL SEGAL