

NOTE:

Note included in this PDF Document are the Exhibits.

You may locate these Exhibits in previous Documents filed

RDW
2000R00769

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Criminal No. 00-404
v. : HON. NICHOLAS H. POLITAN, U.S.D.J.
NICODEMO S. SCARFO, and :
FRANK PAOLERCIO :

SUPPLEMENTAL BRIEF OF THE UNITED STATES
IN OPPOSITION TO DEFENDANT SCARFO'S SUPPLEMENTAL MOTION
TO SUPPRESS THE EVIDENCE SEIZED BY THE GOVERNMENT
THROUGH THE USE OF THE KEY LOGGER SYSTEM

ROBERT J. CLEARY
United States Attorney
970 Broad Street
Newark, New Jersey 07102
(973) 645-2822

On the Brief:

RONALD D. WIGLER
Assistant U.S. Attorney

TABLE OF CONTENTS

PROCEDURAL HISTORY	1
POINT 1	
DEFENDANT'S MOTION TO SUPPRESS SHOULD BE DENIED FOR FAILURE TO MEET HIS INITIAL BURDEN OF PROVING THAT AN UNLAWFUL INTERCEPTION OF AN ELECTRONIC COMMUNICATION WHICH CONTAINED THE PGP PASS PHRASE AND KEY RELATED INFORMATION DID IN FACT OCCUR	4
a. Defendant Carries the Burden of Proving to the Trial Court's Satisfaction that the Evidence Proffered by the Government was obtained as a Result of an Unlawful Wiretap.	4
b. Defendant Has Failed to Prove by a Preponderance That Any Electronic Communication Was In Fact Captured Much Less an Electronic Communication Containing the Defendant's PGP Pass Phrase and Key-related Information	6
POINT 2	
THE UNCLASSIFIED SUMMARY AFFIDAVIT IS SUFFICIENT, TOGETHER WITH OTHER MATERIALS IN THE EXISTING RECORD, TO PERMIT FULL LITIGATION AND APPROPRIATE ADJUDICATION OF THE PENDING DEFENSE MOTION TO SUPPRESS	16
POINT 3	
THE GOVERNMENT'S USE OF THE UNCLASSIFIED SUMMARY AFFIDAVIT DOES NOT POSE A DIRECT CONFLICT WITH THE JENCKS DECISION	24

...table of contents cont'd.

POINT 4

THE COURT ORDERS FROM MAY 8, 1999 AND JUNE 9, 1999
DID NOT CONSTITUTE A GENERAL WARRANT VIOLATIVE OF
THE FOURTH AMENDMENT 30

a. The Key Logger System Required Multiple
Components 30

b. Suppression of the PGP Pass Phrase and
Key-Related Information is not an
Appropriate Remedy 34

CONCLUSION 36

PROCEDURAL HISTORY

On June 21, 2000, a federal grand jury returned a three-count gambling and loansharking Indictment against defendants Nicodemo S. Scarfo and Frank Paolercio.

On June 20, 2001, defendant Scarfo filed a motion for discovery pursuant to Rule 16 of the Federal Rules of Criminal Procedure and a motion to suppress evidence seized through the ~~use of a specialized technique, hereinafter referred to as the~~ "Key Logger System (KLS)." A brief of the United States in opposition to defendant Scarfo's motion was filed with the Court on July 17, 2001. A hearing was held before the Court on July 30, 2001. At the hearing, the Court ordered additional briefing by the parties. Defendant Scarfo's supplemental brief was filed on August 1, 2001, the Government's supplemental response was filed on August 3, 2001. The Court issued a Letter Opinion and Order on August 7, 2001, in which the Court ordered the Government to submit a report detailing how the Key Logger System functions by August 31, 2001. The Court, however, permitted the Government to file with the Court a more particularized explanation of the security concerns which would arise if the Key Logger System technology were publicly disclosed, and any testimonial evidence the Government deemed necessary.

On August 23, 2001, the Government requested that the Court modify its August 7, 2001 Order and permit the Government to

proceed under the Classified Information Procedures Act, [hereinafter "CIPA"], Section 4, 18 U.S.C. App. III, § 4, since disclosure would require divulging classified information. On August 31, 2001, the defense filed its objection to the Government proceeding under CIPA claiming that the Government had failed to demonstrate a sufficient showing that the information concerning the Key Logger System had been properly classified. On September 7, 2001, the Court conducted a hearing to ascertain whether the Government would be able to proceed ex parte, in camera pursuant to CIPA. At the conclusion of that hearing, the Court permitted the Government to proceed under CIPA.

On September 26, 2001, an ex parte, in camera proceeding was held before the Court where the United States sought a Protective Order denying disclosure of classified information and directing in lieu thereof disclosure to the defense of a substitute Unclassified Summary Affidavit.

On October 2, 2001, this Court granted the Government's motion for a Protective Order and ordered that the Government, in lieu of disclosure of the classified information, provide the defense with the substitute Unclassified Summary Affidavit of information, which the Court had determined would be sufficient, together with other materials in the existing record, to permit full litigation and appropriate adjudication of the pending defense motion to suppress.

On October 5, 2001, the United States filed the Unclassified Summary Affidavit, in the form of the "Affidavit of Randall S. Murch" dated October 4, 2001, with the Court and served a copy on counsel for the defense (See Exhibit A).

On November 9, 2001, the United States received via facsimile a copy of defendant Scarfo's undated Memorandum of Law and Supplemental Motion to Suppress Evidence Seized by the Government through the Use of the Key Logger System [hereinafter, "November 9, 2001 Supplemental Motion to Suppress"].

POINT 1

Defendant's Motion to Suppress Should Be Denied
For Failure to Meet His Initial Burden
of Proving That an Unlawful Interception of an
Electronic Communication Which Contained the PGP
Pass Phrase and Key Related Information Did in Fact Occur

Defendant Scarfo's November 9, 2001 Supplemental Motion to
Suppress is another attempt to obtain classified information
concerning the functionality of the Key Logger System. Defendant
~~now asserts that the Unclassified Summary Affidavit is still~~
inadequate to provide the defense, and the Court, with a reliable
assessment of whether or not the Key Logger System captured
electronic communications in violation of Title 18, U.S.C. § 2510
et seq., or more commonly referred to as Title III. The
defendant's assertion is unfounded. The fact of the matter is
that the defendant has completely failed to substantiate his
initial threshold burden of proving that the evidence proffered
by the Government, i.e., the PGP pass phrase and key related
information, was obtained unlawfully.

- a. Defendant Carries the Burden of Proving to the Trial
Court's Satisfaction that the Evidence Proffered by the
Government was obtained as a Result of an Unlawful
Wiretap.

It is a basic tenet of American criminal jurisprudence that
a defendant seeking to suppress evidence must carry at least the
initial burden of proving that the evidence proffered by the
Government was obtained as a result of some illegality. United

States v. Morin, 378 F.2d 472, 475 (2nd Cir. 1967) (defendant's conjecture over the probability that the FBI must have conducted an illegal search of defendant's suitcase is inadequate as "burden of showing unlawful conduct rests on the [defendant]") citing Addison v. United States, 317 F.2d 808, 812 (5th Cir. 1963) ("We think the cases clearly hold that the burden is on the accused attacking the propriety of evidence used against him to establish the fact that it was in fact illegally obtained." (emphasis added.)), cert. denied 376 U.S. 936 (1964); United States v. Arboleda, 633 F.2d 985, 989 (2nd Cir. 1980) (cases cited therein). Where the search was conducted pursuant to a judicially-authorized search warrant, the determination of whether a defendant has met this burden must be viewed in light of the "presumption of validity" which adheres to all searches conducted pursuant to a warrant. United States v. Yung, 786 F. Supp 1561, 1570 (D. KS 1992); United States v. Nunex, 658 F. Supp 828, 835 (D.Co. 1987) citing Samuels v. McCurdy, 267 U.S. 188, 199 (1925); See generally Franks v. Delaware, 438 U.S. 154, 98 S.Ct. 2674 (1979). In cases involving electronic surveillance, the defendant's burden is no less than that required in any other suppression context. United States v. Macaddino, 496 F.2d 455, 459-460 (2nd Cir. 1974) (quoting Nardone et al v. United States, 308 U.S. 338, 341 (1939) ("burden is, of course, on the accused in the first instance to prove to the

trial court's satisfaction that wire-tapping was unlawfully employed."). Typically, the quantum of evidence required to meet the "trial court's satisfaction" is proof by a preponderance. Wiretapping and Eavesdropping, Clifford F. Fishman & Anne T. McKenna, 2nd ed. 1995, pp. 23-8 & 23-47.

Moreover, a person may seek to suppress intercepted conversations or derivative evidence as a violation of Title III only if he is an "aggrieved person,"¹ and he is not entitled to win suppression unless he establishes, based on any of three specified statutory grounds, that the illegality deprived him of his rights. 18 U.S.C. § 2518(10)(a); see United States v. Williams, 580 F.2d 578, 583 (D.C. Cir. 1978), cert. denied 439 U.S. 832 (1978). Here the defendant relies on the ground that he was a party to a communication which was unlawfully intercepted. Thus, he must first prove by a preponderance of the evidence that an electronic communication was in fact intercepted in order to establish his standing.

- b. Defendant Has Failed to Prove by a Preponderance That Any Electronic Communication Was In Fact Captured Much Less an Electronic Communication Containing the Defendant's PGP Pass Phrase and Key-related Information.

The defendant's suggestion that some text, not sought to be

1. An "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed. 18 U.S.C. § 2510(11).

introduced into evidence by the Government, could potentially be part of an electronic communication is not an adequate showing that an unlawful interception had in fact occurred. The defendant acknowledges that the United States provided him with documentation which the Government has repeatedly identified as the total output, that is, represents the total capture of the Key Logger System. See "Supplemental Brief of Defendant Nicodemo S. Scarfo," undated (filed on or about August 1, 2001) and

Attachment A. However, to date the defendant has not identified by sworn affidavit or otherwise any of the specifics relating to the alleged electronic communications which he suggests may have been intercepted. The defendant has not identified the recipient of the communication, the approximate date or time of its transmission, or mode of transmission (e-mail, instant message, etc.). Nor has the defendant even averred that he was, in fact, the author of any such electronic communication. In lieu of an affirmative showing, the defendant merely points to a reference in the Key Logger System output to "eyeglasses"² and, in effect, boldly asserts that this reference could have been part of an electronic communication. See "Supplemental Brief of Defendant Nicodemo S. Scarfo," undated (filed in August 2001), at pp. 4, 9 (The eyeglasses reference "has to be or is very likely" an

2. This reference to eyeglasses appears on page 22 of the Key Logger System output.

electronic communication; the eyeglasses reference is an "indication" that at least one electronic communication was captured).

The United States strongly disputes this unsubstantiated defense assertion. The more plausible explanation for the capture of the keystrokes related to "eyeglasses" is most logically supported by the other text surrounding it. That is, just prior to the "eyeglasses" notation in question, the "keystroke capture" component recorded "LotusOrganizer"³ followed by "WinwordDocs1." Then, the words, "The Classic Eye Glasse Caddy," is recorded. This is followed by other keystrokes, "ggkLLJK" and only then is there the text of the notation concerning eyeglasses. Given the preceding entries, the "eyeglasses" text noted by the defense appears to be a "note" from Scarfo to himself, which is completely consistent with notations normally inputted when one uses a program such as Lotus Organizer, or perhaps stored in file document form on the computer's hard drive.

It would be the odd circumstance that any computer search pursuant to warrant would not seize cognizable text, but the bare existence of such text does not render it an electronic

3. "Lotus Organizer" is an electronic organizer program designed to allow the user to input personal information, call logs, and other important productivity notes. Included in the basic package are usually sections for a notepad as well as a journal.

communication. Even more to the point, the defendant has utterly failed to offer any evidence that the PGP pass phrase and key-related information, which is the only information captured by the Key Logger System which the Government seeks to utilize, was part of any electronic communication, much less part of the suggested "eyeglasses" communication. The intercept prohibitions of Title III upon which the defendant relies so heavily, do not apply to transmissions wholly internal to defendant's computer.

Cf. United States v. Peoples, 250 F.3d 630, 636 (8th Cir. 2001) (communications over internal telephone-like system in prison visitor room lacked requisite interstate nexus and were therefore not protected by Title III).

In response to the Government's filing of the Unclassified Summary Affidavit, the defendant argues, in substance, that he should not be forced to rely upon the representations of the Government. In essence, the defendant argues that he requires additional discovery, namely access to the Key Logger System itself and other technical materials, in order to determine for himself whether the Key Logger System did, or could have, intercepted his electronic communications, if even as a result of malfunction.⁴ See Exhibit B - defendant's "Affidavit of David J.

4. "It is impossible to determine if there were any safeguards in the event of a malfunction of one or more of the procedures [of the Key Logger System]." Affidavit of David J. Farber at p. 2. The defendant's reference to the need to evaluate even the

(continued...)

Farber," at p.2, 6-7, dated by reference of accompanying Declaration of November 8, 2001 ("Blind acceptance" of Murch assertions are unacceptable). But a defendant's failure to make an initial showing of illegality in support of his motion to suppress can not serve as the basis for additional discovery where there exists a legitimate and significant government interest against unnecessary disclosure and the courts have been quick to reject such bootstrapping arguments for expanded discovery in cases involving electronic interceptions. See United States v. Williams, 580 F.2d 578 (D.C. Cir. 1978), cert. denied 439 U.S. 832 (1978) and cases cited therein at n.38; In re U.S. 564 F.2d 19, 23 (2nd Cir. 1977) (defense request for disclosure of identity of informant generating probable cause, even under a pledge of secrecy, would authorize an unnecessary rummaging in the government's files and would compromise the fundamental public policy underlying the informer privilege.).

In United States v. Williams, *ibid.*, defendants claimed that the wiretaps conducted by the Government in 1974 which led to their indictment on gambling charges were tainted by nine admittedly illegal wiretaps conducted from 1969 through 1973. The defendants argued that it was likely that the Government had

4. (...continued)

effect of potential Key Logger System malfunctions, in the utter absence of even a scintilla of evidence of any malfunction, truly demonstrates the speculative nature of his discovery request in the face of his failure to meet his initial burden.

used information derived from the illegal 1969-1973 wiretaps to cultivate confidential informants and gain other information which contributed to the probable cause for the 1974 interceptions. In support of their motions to suppress the 1974 interception recordings by establishing standing, defendants filed affidavits explicitly averring that they had called one or more of the telephone numbers of the subjects/premises of the 1969-1973 wiretaps during the relevant period, spoken to the subjects, and therefore, expected to be recorded on the illegal interceptions. In response, the Government affirmatively denied pursuant to Title 18, U.S.C. § 3504⁵ that the defendants had been

5. 18 U.S.C. § 3504 provides:

(a) In any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority of the United States-

(1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act;

(2) disclosure of information for a determination if evidence is inadmissible because it is the primary product of an unlawful act occurring prior to June 19, 1968, or because it was obtained by the exploitation of an unlawful act occurring prior to June 19, 1968, shall not be required unless such information may be relevant to a pending claim of such inadmissibility; and

(3) no claim shall be considered that evidence of an event is inadmissible on the ground that such evidence was obtained by the exploitation of an unlawful act

(continued...)

intercepted in any of the 1969-1973 illegal interceptions. Undaunted, the defendants filed motions for additional discovery of the tapes and transcripts of the 1969-1973 interceptions. In affirming the district court's denial of the defendant's request for discovery and motion to suppress, the United States Court of Appeals for the D.C. Circuit emphasized:

[I]t is well settled that an accused has "no right to rummage in government files," and that to "elicit () what is in the Government's possession before its submission to the jury" he "must satisfy the trial court with (the) solidity" of his claim. Put another way, "tenuous claims (are not) sufficient to justify the trial court's indulgence of inquiry into the legitimacy of evidence in the Government's possession." We have, then, hewed to the view that the Government's denial must generally be accepted as conclusive, and we do so again today.

Williams, Ibid. at 582. (Citations omitted.)

Accordingly, in the absence of demonstrable evidence of an unlawful act, a defendant is not entitled to full discovery for resolution of every issue relating to electronic surveillance merely to confirm for himself that a violation did not or could

5. (...continued)

occurring prior to June 19, 1968, if such event occurred more than five years after such allegedly unlawful act.

(b) As used in this section "unlawful act" means any act the use of any electronic, mechanical, or other device (as defined in section 2510(5) of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto.

not have occurred. Taglianetti v. United States, 394 U.S. 316 (1969) (per curium) (defendant is not entitled to additional wiretap logs and tapes merely to confirm that Government had not omitted recordings in discovery through failure to properly identify defendant's voice especially where the district court had inspected the additional materials in camera).

The United States respectfully submits that this Court should reject defendant Scarfo's meager representations regarding the existence of any electronic communication which was intercepted as insufficient to meet his initial burden of demonstrating an unlawful act. The defendant has provided no explanation from which the court could reasonably conclude that merely because text relating to "eyeglasses" was seized by the Key Logger System, that this text was part of an electronic communication transmitted in real time and was not part of any other static document which was typed and saved on the computer without transmission. The search of the defendant's computer was conducted pursuant to a valid, judicially-authorized search warrant, and is presumed to be a lawful search. The Government has provided in the Unclassified Summary Affidavit sufficient detail as to the methodology of the Key Logger System to support the conclusion that the search was and could be conducted without intercepting any electronic communications from the defendant's computer. In essence, the Unclassified Summary Affidavit

represents a detailed denial by the Government under 18 U.S.C. § 3504 of any unlawful act relative to the seizure of the PGP pass phrase and key-related information. The defendant has not submitted under oath any evidence supporting a finding by a preponderance that: 1) he was the author of one or more electronic communications during the relevant period; 2) there were in fact any electronic communications during the relevant period, including mode of communication (instant message, e-mail, etc.), name of the recipient, date and/or time and subject matter;⁶ 3) that such communications were transmitted in real time (versus having first been saved off-line and subsequently transmitted); and 4) that such communications contained the PGP pass phrase and key-related information which the Government now

6. Even assuming that the defendant was, by affidavit, to credibly identify some portion of the Key Logger System output, provided in discovery, which was allegedly part of a contemporaneously transmitted outgoing electronic communication, any remedy the Court would choose to fashion should apply only to that portion of the Key Logger System output and would not include the encryption pass phrase unless the defendant can demonstrate that the PGP pass phrase and key-related information were part of that communication. See Wong Sun v. United States, 317 U.S. 471 (1963); United States v. Charles, 213 F.3d 10, 21-22 (1st Cir. 2000) (affirming trial court's partial suppression remedy for violation of minimization order in wiretap) cert. denied, Charles v. United States, 531 U.S. 915.

In the case of improperly intercepted electronic communications, however, Congress has purposefully omitted a suppression remedy. See 18 U.S.C. § 2515 (limiting suppression to wire and oral communications, but not electronic communications). A more comprehensive discussion of this issue is contained in the Government's July 17, 2001 Brief in Opposition to Defendant's Pretrial Motions, pp. 30-32.

seeks to utilize in introducing evidence against him. In the absence of such a showing, the defendant has failed to meet his burden and his motion to suppress should be denied without further action.

POINT 2

The Unclassified Summary Affidavit Is Sufficient,
Together with Other Materials in the Existing Record,
to Permit Full Litigation and Appropriate Adjudication
of the Pending Defense Motion to Suppress

Pursuant to the Protective Order signed by this Court on October 2, 2001, the United States provided the defense with an Unclassified Summary Affidavit. Prior to signing the Protective Order, this Court, in accordance with CIPA § 4, and Federal Rule of Criminal Procedure 16(d)(1), received ex parte, in camera, several documents, including a Memorandum of Law and supporting Affidavits, along with Oral Testimony, which sufficiently demonstrated to this Court that: (1) none of the material sought to be protected by the Government constituted Brady material; and (2) the Unclassified Summary Affidavit, together with other materials in the existing record, permit full litigation and appropriate adjudication of the pending defense motion to suppress.

Defendant Scarfo now asserts in his November 9, 2001 Supplemental Motion to Suppress, pp. 2,3 that the Unclassified Summary Affidavit is "inadequate to provide this Court or the defense with a reliable assessment of whether the KLS did or did not capture electronic communications (email, instant messaging) because of its extreme vagueness and its lack of an adequate foundation on which to base the conclusions it forwards." The defense's argument is derived from the raw conclusions proffered

in the Affidavit of David J. Farber.

In turn, Mr. David J. Farber arguments may, in essence, be distilled to the following points:

1. VERIFICATION BY THE DEFENSE.

Dr. Murch's Unclassified Summary Affidavit is allegedly inadequate because it fails to provide sufficient detail to allow Mr. Farber "to determine [for himself] whether the KLS operated as claimed." Affidavit of David J. Farber at p.2, para.9, dated by reference of accompanying Declaration of November 8, 2001.

In order for the defense to verify the factual representations made by Dr. Murch, and exclude the possibility of any interception of electronic communications, whether caused by malfunction or otherwise, additional discovery is necessary, including, but not limited to:

- i. The "procedures, software utilities and the actual [Scarfo] computer[;]" - Farber Affidavit, id.;
- ii. "[T]he particular version of PGP, as configured on that computer;" - Farber Affidavit, id. at p.4, para.14.
- iii. "[A] copy of any data that was removed from the [Scarfo] computer[;]" Farber Affidavit, id. at p.6, para.17.
- iv. "The specifications of any additional software, hardware and/or firmware that was used to evaluate, remove and/or analyze data from the [Scarfo] computer[;]" Farber Affidavit, id.

- v. "The actual [Scarfo] computer that the government installed the KLS on." Farber Affidavit, id.

2. THE POSSIBILITY OF KLS INTERCEPTION CAUSED BY UNSPECIFIED HYPOTHETICAL MALFUNCTIONS:

Dr. Murch's Unclassified Summary Affidavit is allegedly inadequate because it fails to describe "if there were any safeguards in the event of a malfunction of one or more of the procedures of the [KLS]," Farber Affidavit, id. at p.2, para.8, or how the KLS would deal with "commonly available counter measures [which might have been] present [and which, if present] would disable the system if a foreign agent (program or device) [e.g. the KLS] were installed on [the Scarfo computer]." Farber Affidavit, id. at p.3, para.9.

3. THE POSSIBILITY OF KLS INTERCEPTION RESULTING FROM THE POSSIBLE INSTALLATION IN THE COMPUTER OF OTHER COMMUNICATIONS DEVICES:

Dr. Murch's Unclassified Summary Affidavit is allegedly inadequate because it is premised upon the existence of only one communications device, namely a modem, and does not address the possibility of other communications devices "such as a network card, prior to, during or after installation and operation of the KLS." Farber Affidavit,

7. Mr. Farber appears to be unaware that the Scarfo computer, which he demands to examine as a critical element in his evaluation of the KLS (see Farber affidavit at paragraphs 9, 11, 14, and 17), is not in the Government's possession. Indeed, the FBI did not take physical possession of defendant Scarfo's computer or hard drive.

id. at p.3, para.11.

4. PERCEIVED INCONSISTENCIES IN THE MURCH STATEMENT:

Dr. Murch's Unclassified Summary Affidavit is allegedly inadequate because of alleged inconsistencies in the Summary Affidavit. See. e.g. Farber Affidavit, id. at p.3, para.10, 12.⁸

In response, the Government submits that Dr. Murch's Unclassified Summary Affidavit does, in fact, "provide this Court [and] the defense with a reliable assessment of whether the KLS did or did not capture electronic communications," by succinctly disclosing, amongst other facts, the following:

1. The Key Logger System will typically have multiple components. Affidavit of Randall S. Murch dated October 4, 2001 at p.5, para.4. A component of the KLS deployed in

8. While incorrectly re-stating it, Mr. Farber takes great exception to Dr. Murch's assertion that, in a Microsoft Windows environment, a user could be operating a word processing application in one window without [necessarily] transmitting an electronic communication, while a different application utilizing the modem could be operating in another inactive window. Given that the Scarfo computer is in the possession of the defense, Mr. Farber should have known that the defendant was using AOL 3.0 for his Internet access. Knowing this, Mr. Farber should also have known, for various reasons, that AOL 3.0 is incompatible with MS Outlook. Plainly stated, even if the defendant used MS Word as his editing software for Microsoft Outlook, MS Word would still be incapable of accessing the Internet, as stated in the Murch Affidavit, since it is a well documented fact that Microsoft Outlook will not work with AOL 3.0. This is documented at: "<http://support.microsoft.com/support/outlook/tshooters/sendrec2a.asp>". Therefore, the scenario that Mr. Farber outlined is impossible.

this case was the "keystroke capture" component, Murch Affidavit, id. at pp.5,6, para. 6, and a mechanism was developed "to record the passphrase as entered via the keyboard by the user and certain other key-related information," Murch Affidavit, id. at p. 8, para. 10. "Other than the output that was captured by the keystroke component, . . . , the only other output captured by the other component(s) was/were the last three lines of the last page of that combined output, which captured the passphrase and key-related information." Murch Affidavit, id. at p. 10, para. 12. Examination of the Scarfo computer revealed that it had a modem and "that [Scarfo's computer] possessed no other common or recognizable means of communicating with other computers [i.e. transmitting electronic communications] except through the modem" "connected to a communications port [of the computer]." Murch Affidavit, id. at p.6, para. 6.

2. The "keystroke capture" component was configured in such a way that the default was not to record unless all communications ports were evaluated and determined to be inactive prior to the recording of each individual keyboard keystroke. Murch Affidavit, id.
3. The other component(s) was/were configured in such a way as to determine when the PGP program was in use and record the

[PGP] pass phrase as entered via the keyboard by the user together with other key-related information. Murch Affidavit, id. at pp.7,8, para. 8-10.

In comparison, Mr. Farber's affidavit does nothing to impeach any of the critical factual representations outlined above as stated by Dr. Murch. Mr. Farber's affidavit is more noteworthy for what it fails to address than what it addresses.

Mr. Farber does not deny that the computer had a modem or that modems are connected to communications ports. Mr. Farber does not explain how a computer with only a modem could transmit an electronic communication if there were no activity on any communication port. Instead, Mr. Farber complains only that it is possible that the computer could, hypothetically, have had other means of communications such as a network card.⁹ Farber Affidavit, id. at p.3, para. 11.

Moreover, Mr. Farber does not refute Dr. Murch's factual representation that all of the PGP program's actions involving either encryption or decryption necessarily occurred only within the computer and not on some other networked computer connected via modem as a result of an electronic communication. Murch

9. Indeed, given the fact that the computer in question was not seized by the government and is even at this moment ostensibly still in the possession of the defendant, it is noteworthy that Mr. Farber did not allege that there was any evidence, in fact, supporting the presence of a network card, only that, in theory, one could have existed.

Affidavit, id. at p.8, para.8. Specifically, Mr. Farber does not explain to the Court how the capture of the PGP passphrase as entered by the user in response to prompting by the PGP program, would, at that moment, be the capture of an electronic communication when that capture relates entirely to a function occurring only within the confines of that computer.

Mr. Farber does complain that Dr. Murch allegedly failed to explain what safeguards were put in place in the KLS to address malfunctions of the computer. However, Mr. Farber, while alleging the broken "6" key, Farber Affidavit, id. at p.4, para.15, does not even allege that this malfunction would in fact have affected either the "keystroke capture" component¹⁰ or any other component(s) so as to cause the capture of electronic communications.

In a similarly unresponsive manner, Mr. Farber suggests that all that was necessary "was to install software that only loaded when PGP was loaded," Farber Affidavit, id. at p.5, para.16. However, Mr. Farber fails to address Dr. Murch's explanation that the "keystroke capture" component and the other component(s) was/were designed to complement each other's shortcomings and were necessary in order to guard against the use of PGP in combination with a wide array of encoding, scrambling or other

10. If anything, it is just as reasonable to conclude that the inoperability of the "6" key would have resulted in the non-capture by the keystroke capture component of the "6" key.

encryption programs¹¹ which would produce encryption layers.

Murch Affidavit, id. at pp.8,9, para 10.

More to the point, Mr. Farber failed to demonstrate that the factual representations of Dr. Murch relating to the configuration and operation of the Key Logger System are in any way false or flawed. Hidden behind the veil of numerous hypotheticals, the gravamen of Mr. Farber's affidavit is not that the KLS could not have properly operated as described by Dr.

Murch, but rather, that Mr. Farber did not have sufficient information to confirm for himself that it could have. Stated differently within the context of the defendant's initial burden in a motion to suppress, Mr. Farber failed to demonstrate that the PGP pass phrase and key-related information was, in fact, acquired as a result of the interception by the KLS of an electronic communication. Essentially un-impeached, the Murch Unclassified Summary Affidavit clearly provides the Court with sufficient detail as to the methodology of the Key Logger System to support the conclusion that the search was and could be conducted without intercepting any electronic communications from the defendant's computer.

11. Since the defendant had ready access to the Internet, the FBI had to provide for the contingency that he would download and use additional data protection and scrambling software not on the system at the time of the original deployment of the KLS.

POINT 3

The Government's Use of the Unclassified
Summary Affidavit Does Not Pose a
Direct Conflict with the Jencks Decision

The Government's obligation to produce and disclose information in the course of the criminal discovery process, although substantial, is a qualified, rather than absolute obligation. In this regard, CIPA § 4, and Rule 16(d)(1), Federal Rules of Criminal Procedure, expressly provide that upon a sufficient showing by the Government of the existence of a legitimate national security privilege, the Government may substitute an unclassified summary of the relevant facts in lieu of the disclosure of classified national security information.¹²

12. CIPA, Section 4 provides:

Discovery of classified information by
defendants

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be

(continued...)

The cases relied upon by the defense in alleging and arguing that the Unclassified Summary Affidavit provided to the defense pursuant to this Court's Protective Order, is inadequate, namely, Jencks v. United States, 353 U.S. 657 (1957), United States v. Andolschek, 142 F.2d 503 (2d Cir. 1944), and Roviaro v. United States, 353 U.S. 53 (1957), each recognize the qualified nature of the Government's obligation to disclose information to the defense. None of the cited cases adopts the apparent position of the defense that the Government has an unqualified obligation to disclose to the defense in a criminal proceeding all information in its possession, regardless of the degree of relevance of the information at issue or competing interests of the parties.

12. (...continued)

sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

Rule 16(d)(1), Fed. R. Crim. P., provides:

Protective and Modifying Orders. Upon a sufficient showing the court may at any time order that the discovery or inspection be denied, restricted, or deferred, or make such other order as is appropriate. Upon motion by a party, the court may permit the party to make such showing, in whole or in part, in the form of a written statement to be inspected by the judge alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the party's statement shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

In determining the scope of the discovery rights of the defense and conversely to the Government's disclosure obligations, the courts have universally recognized that in cases in which it asserts the existence of a valid privilege the Government need only disclose to the defense information that satisfies both requirements of a two-pronged test: (1) the information at issue must be "relevant and helpful to the defense," including information determined to be exculpatory, United States v. de los Santos, 810 F.2d 1326, 1331 (5th Cir.) (quoting Roviaro, 353 U.S. 53, 60-61 (1957)), cert. denied, 484 U.S. 978 (1987); Yunis, 867 F.2d at 622-25 (quoting Roviaro, 353 U.S. at 60-61); and (2) the defendant's interests in obtaining access to the information at issue outweigh the Government's interest in maintaining the secrecy of the material. See also United States v. Pringle, 751 F.2d 419, 426, 428 (1st Cir. 1984) (quoting Roviaro, 353 U.S. 53); and United States v. Gutierrez, 931 F.2d 1482, 1489-92 (11th Cir.) (containing a detailed discussion of Eleventh Circuit's application of the Roviaro balancing test), cert. denied, 502 U.S. 916 (1991).

Determinations of relevance within the meaning of both Rule 16 and CIPA § 4 fall within the trial court's discretion. United States v. Scarpa, 897 F.2d at 70 (Rule 16), cert. denied, 498 U.S. 816 (1990); Yunis, 867 F.2d at 622 (CIPA § 4); Clegg, 740 F.2d at 18 (CIPA § 4).

The CIPA was not . . . intended to expand the traditional rules of criminal discovery under which the government is not required to provide criminal defendants with information that is neither exculpatory nor, in some way, helpful to the defense. See Fed. R. Crim. P. 16; United States v. Yunis, 867 F.2d 617 (D.C. Cir. 1989).

United States v. Varca, 896 F.2d 900, 905 (5th Cir.), cert. denied, 498 U.S. 878 (1990). See also United States v. Anderson, 872 F.2d 1508, 1514 (11th Cir.) (court reviewing CIPA issues must use existing standards for determining relevancy), cert. denied, 493 U.S. 1004 (1989).

Both CIPA § 4 and Rule 16(d)(1) explicitly contemplate that in cases such as those involving classified national security information, the determination of the adequacy of the Government's proposed substitute summary disclosure is to be made by the Court in an ex parte, in camera proceeding.¹³ Such ex parte, in camera proceedings to resolve discovery issues related to a privilege being asserted by the Government have been recognized and approved by the Courts.¹⁴

13. Proceeding ex parte and in camera does not offend the defendant's Sixth Amendment right to confrontation. United States v. Joliff, 548 F. Supp. 229, 231-32 (D. Md. 1981). It follows, as well, that denial of discovery of materials under CIPA § 4 does not deny a defendant's Fifth Amendment right to a fair trial or Sixth Amendment right to confront witnesses. United States v. Porter, 701 F.2d 1158, 1162 (6th Cir.), cert. denied, 464 U.S. 1007 (1983).

14. See, e.g., In re Grand Jury Proceedings in the Matter of Freeman, 708 F.2d 1571, 1576 (11th Cir. 1983) (in camera proceedings appropriate vehicle for resolution of issues of privilege); United States v. Sarkissian, 841 F.2d 959, 965;

(continued...)

As reflected in the Court's Protective Order, the Government appeared before the Court ex parte and in camera pursuant to its earlier filed Motion for a Protective Order. On the basis of that proceeding, this Court found that the Government had made a sufficient showing to authorize the requested Protective Order, and after specific review, this Court also found that none of the material sought to be protected by the Government in the requested use of a substitute Unclassified Summary Statement constituted material subject to disclosure under Brady v. Maryland, 373 U.S. 83 (1963). In granting the Government's motion, and without ruling in any way on the pending defense motion to suppress, this Court ordered "that the Government . . . provide the defense with the substitute Unclassified Summary Statement . . . which the Court has determined would be sufficient, together with other materials in the existing record,

14. (...continued)

United States v. Lee, 648 F.2d 667, 668 (9th Cir. 1981) ("[i]n camera submissions are proper to evaluate government claims regarding national security"); United States v. Kampiles, 609 F.2d 1233, 1248 (7th Cir. 1979) ("[i]t is settled that in camera, ex parte proceedings to evaluate bona fide national security information are proper"), cert. denied, 446 U.S. 954 (1980). In a similar vein, courts have explained that the very purpose of seeking a protective order under Rule 16(d)(1) would be lost in certain instances if the application were not pursued ex parte and in camera. United States v. Pelton, 578 F.2d 701, 707 (8th Cir.) ("[a]n adversary proceeding would have defeated the very purpose of the requested order by revealing [the witnesses'] identities to [the defendant]"), cert. denied, 439 U.S. 964 (1978); In re Taylor, 567 F.2d 1183, 1187-89 (2d Cir. 1977) (in camera, ex parte proceedings serve to resolve conflict between defendant's rights to discovery and Government's claim of privilege).

to permit full litigation and appropriate adjudication of the pending defense motion to suppress. . . ."

The Government respectfully submits that the defense contention that the Government has failed to comply with the requirements of CIPA and/or the ruling in Jencks, supra, is without merit. Rather, as determined by this Court in its earlier Order, the Government has observed its discovery obligation related to the pending defense motion to suppress by providing to the defense the Unclassified Summary Affidavit. This Unclassified Summary Affidavit, together with other information of record, fully satisfies any legitimate interests of the defense in having access to information within the possession of the Government relevant and material to litigation and adjudication of the pending motion to suppress. To impose upon the Government additional disclosure requirements as suggested by the defense would render meaningless the legitimate qualified privilege of the Government to protect the national security interests of the United States under the Classified Information Procedures Act, the Federal Rules of Criminal Procedure, and the Federal Rules of Evidence.

POINT 4

The Court Orders from May 8, 1999 and
June 9, 1999 Did Not Constitute a
General Warrant Violative of the Fourth Amendment

The defendant has again alleged in his November 9, 2001 Supplemental Motion to Suppress that the May 8, 1999 Court Order and the June 9, 1999 Court Order, which authorized the capture of every keystroke, constituted an unconstitutional general warrant.

~~Defendant now asserts that since the Government had the~~ capability to only capture keystrokes relevant to the "pass phrase," the Government need not have captured all of the keystrokes. Therefore, the Government by not limiting its information gathering ability to the "pass phrase only" component, invited, and received, an unnecessary over collection of data. Defendant Scarfo's characterization of the two Orders is still mistaken and the allegation is without merit.¹⁵

a. The Key Logger System Required Multiple Components

The F.B.I. recognized that there was an inherent weakness in using only the "keystroke capture" component of the Key Logger System. The inherent weakness was due to the fact that in a "multi-tasking" environment associated with a Microsoft Windows

15. In order to avoid redundancy, the United States incorporates by reference its prior submissions concerning why the May and June 1999 Orders did not constitute general warrants in violation of the Fourth Amendment which are contained in its July 17, 2001 Brief in Opposition to Defendant's Pretrial Motions, pp. 33-47; and in its August 3, 2001 Letter Brief, pp. 8-12.

operating system (which was the operating system on defendant's computer), it is possible for an individual or user to connect his computer to the Internet and cause that operation to take place in the "background" in one window, and then operate other applications on his system (e.g., word processing, spreadsheet, etc.) at the same time in another window.¹⁶ Performing word processing in one window application, while the modem is activated in another window application would have no bearing on Title III implications as to the word processing work performed by the user or individual. Under such a scenario, involving concurrent multi-tasking applications, the defendant could have used his PGP program to decrypt files stored on his computer while the modem was activated in the background, and the "keystroke capture" component would not have recorded the defendant's pass phrase.

In an effort to combat this inherent weakness, the F.B.I. developed a mechanism to record the pass phrase as entered via the keyboard by the user and certain other key-related information. This mechanism worked as a complement to the "keystroke capture" component of the Key Logger System.

The F.B.I. also recognized that it was possible for the defendant to use PGP in sequential combination with a wide array

16. It has become more common for computer users to continuously stay on line in order to avoid "dial up" or connection times as internet service providers permit unlimited access.

of encoding, scrambling or other encryption programs which would produce encryption layers. Such a process would effectively prohibit recovery of cognizable plain text even if the PGP pass phrase and key-related information were captured. Under these circumstances, the "keystroke capture" component would provide necessary capture capability to guard against this and other unknown contingencies.

The Unclassified Summary Affidavit provided to the defense discussed at length the need and logic in employing multiple components in the Key Logger System. The Murch Affidavit specifically asserted that "the KLS, depending upon the hardware and software configuration of a targeted computer and use of the computer, can, and typically will, have multiple components." Murch Affidavit, p. 5, para. 4.

The requirement for multiple components in this case was necessitated in direct response to the specific configuration of the defendant's computer. It was known that the defendant's computer utilized a modem. It was also known that the computer contained a specific encryption program known as PGP and other applications capable of being used to encrypt and/or password protect data or files, thus affording the user the capability to utilize a multi-layered protection scheme. The requirement in this instance for multiple components was based upon the configuration and use of the defendant's computer wherein it was very likely that the computer would use a modem through which to

connect to an Internet Service Provider (ISP) and was capable of multi-layered encryption or security techniques.

The other applications on the defendant's computer, capable of being utilized to encrypt or password protect stored data or files, which included Microsoft Office Pro 95 (which included Word, a word processing application; Excel, a spreadsheet application; and Access, a database application), PKZIP version 2.04g, WinZip 6.1, as well as Quickbooks 5.0.4.1, clearly

indicated the very real capability for the defendant to utilize multi-layering security to protect his alleged criminal activity. Thus, the limitation of the "keystroke capture" component with respect to its operation while the computer is connected to an ISP, necessitated the multi-components in order to ensure that the court ordered search could be effective as well as limited in its scope.

The Government's concern that the defendant would utilize multiple layers of encryption was in fact borne out as the defendant in attempting to protect at least one "factors" file employed both PGP encryption and the Excel application's password protection scheme.

Accordingly, the multiple components of the Key Logger System complemented each other, while operating within the parameters of the May 8, 1999 and June 9, 1999 Court Orders, specifying that the Key Logger System would not be used in conjunction with the computer's modem, thus not capturing

communications subject to Title III protection.

b. Suppression of the PGP Pass Phrase and Key-Related Information is not an Appropriate Remedy

The Third Circuit has previously recognized that there are appropriate limitations on the application of the exclusionary rule. Thus, even if, *arguendo*, the capture of the non-password information exceeded the proper bounds of a warrant, suppression of the pass phrase and key-related information would not be a suitable remedy since these items were precisely the items sought in the two Orders.

In United States v. Christine, 687 F.2d 749 (3d Cir. 1982), the Third Circuit noted that "[w]ithout exception federal appellate courts have held that only that evidence which was seized illegally must be suppressed; the evidence seized pursuant to the warrant has always been admitted." 687 F.2d at 757; *See also United States v. Harcus*, *supra*, 128 F.3d at 1363; United States v. Coleman, 805 F.2d 474, 483 (3d Cir.1986) (same); United States v. Dunloy, 584 F.2d 6, 11 n.4 (2d Cir. 1978); United States v. Forsythe, 560 F.2d 1127, 1134 (3d Cir. 1977); United States v. Mendoza, 473 F.2d 692, 696 (5th Cir. 1972).

Further, the Third Circuit in Christine, stated that "[t]he entire search would only seem to be invalid if its general tenor was that of an exploratory search for evidence not specifically related to the search warrant." 687 F.2d at 757 (quoting from United States v. Russo, 250 F. Supp. 55, 58 (E. D. Pa. 1966)).

Suppression is particularly unwarranted in the instant case since the Government has no intention of seeking admission of the non-password material. If, arguendo, there were any substance to the view that the non-password information could have been the unspoken subject matter of the search, and if the government had in fact sought to utilize or introduce any of the non-password information in this case, then at least there might be some plausible basis for the defense to seek suppression of that information. However, that is not the case here. Rather, the only item that the government has made use of is precisely the information that was the particularly-described subject matter of the two Orders, i.e. the defendant's PGP pass phrase and key related information. Indeed, the pass phrase itself has no intrinsic, substantive evidentiary value. Like a key, it merely serves mechanically (here electronically) to open a container wherein the actual evidence (the "Factor" files) resides. Accordingly, the defense motion to suppress is not warranted.

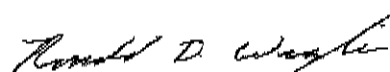
For all of the above reasons, since the May 8, 1999 Order and the June 9, 1999 Order cannot be characterized as a general warrant in violation of the Fourth Amendment, defendant's motion to suppress the evidence seized should be denied.

CONCLUSION

The United States respectfully submits that the Court should deny defendant's motion to suppress.

Respectfully submitted,

ROBERT J. CLEARY
United States Attorney



By: RONALD D. WIGLER
Assistant U.S. Attorney

Newark, New Jersey
December 3, 2001