UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	CRIMINAL NO. 00-00-404
V.	:	TITLE 18 U.S.C SECTIONS 894, 1955, and 2
NICODEMO S. SCARFO	:	

MEMORANDUM OF LAW AND SUPPLEMENTAL BRIEF OF DEFENDANT NICODEMO S. SCARFO

VINCENT C. SCOCA, ESQUIRE
Counsel for Nicodemo S. Scarfo
55 Washington Street
Bloomfield, NJ 07003

NORRIS E. GELMAN, ESQUIRE
Co-Counsel for Nicodemo S. Scarfo
The Public Ledger Building
620 Chestnut Street
Suite 940
Philadelphia, PA. 19106

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	CRIMINAL NO. 00-00-404
v.	:	TITLE 18 U.S.C. SECTIONS 894, 1955, and 2
NICODEMO S. SCARFO	:	

SUPPLEMENTAL MOTION TO SUPPRESS EVIDENCE SEIZED BY THE GOVERNMENT THROUGH THE USE OF A KEYSTROKE RECORDER

Comes now, Nicodemo S. Scarfo, by and through his legal counsel Vincent Scoca, Esquire and co-counsel Norris E. Gelman, Esquire requesting suppression in accordance with this Motion and a hearing thereon. In support thereof he states:

1. Sometime after January 15, 1999 the government searched what it called the targeted computer on which it found an encrypted file. Thereafter, the government found it could not open this file because it was encrypted and such files can only be opened by use of a password and/or a key. This file is hereinafter referred to as Factors January.

2. On May 8, 1999 United States Magistrate Judge G. Donald Haneke entered an Order permitting F.B.I. Agents to "install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on Nicodemo S. Scarfo's computer in the TARGET LOCATION so that the F.B.I. can capture the password necessary to decrypt computer files by recording the key related information as they are entered."

This warrant was renewed again in June of 1999.

According to the Summary provided on October 4, 2001 by Special Agent Randall S. Murch of the FBI's Laboratory Division a "passphrase" was recorded on or before May 23, 1999 and retrieved sometime in June 1999. (Summary, pg. 10, paragraphs 13

and 14).

This passphrase would not open the January Factors encrypted file which was the object of the search warrants.

On July 15, 1999 a physical raid on the defendant's home resulted in the seizure of three other files called Factors, Factors 2 and Factors 3. The government found that the passphrase it had previously secured by the May and June Search Warrants opened all three Factors files seized in July - but did not open the January Factors file.

3. Defendant Nicodemo S. Scarfo alleges that proceeding by way of a search warrant to secure the right to install and capture all or some key strokes on the target computer's keyboard was improper. He further alleges that Title III had to be invoked and followed before such an invasion and seizure from the defendant's office computer could be accomplished. See Title 18, U.S.C. Sections 2510 et seq. He incorporates by reference herein his previous Suppression Motion and Memorandum in Support thereof as to his alleged Title III violations and as to his position that even if proceeding by Search Warrant is found to be proper, the Warrant that issued and which was executed was a General Warrant prohibited by the Fourth Amendment.

4. On, October 2nd, 2001, this Court granted the Government's Motion to Proceed under CIPA and allowed the Government to produce a summary covering the key logger system ("KLS") in question. The Court later found this Summary to be adequate under CIPA so as to allow further proceedings.

I. THE MURCH SUMMARY IS INADEQUATE UNDER CIPA.

5. Defendant Scarfo seeks to show in this proceeding that the Summary provided on October 4, 2001 by Supervisory Special Agent Randall S. Murch of the FBI's Laboratory Division as a Deputy Assistant Director 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. (See attached Affidavit from Dr. David Farber which is Exhibit "1", pg. 5 - "This summary is inadequate for me, or for anyone knowledgeable in the computer field, to be able to ascertain with the requisite degree of scientific certainty that the KLS did not intercept or capture electronic communciations (email, instant messaging, etc."; Conclusion - "The summary provided by Randall S. Murch is insufficient because it is written in such a manner that it is capable of various meanings, which can only be clarified by an explanation of the operation of the key logger.").

The Summary does not "provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information." See CIPA, 18 App. Section 6 (1)(c)((1).

Accordingly, under CIPA, this Court may either order the government to provide the defense with the operation of KLS or of the items requested by Dr. Farber in paragraph 17 of his Statement.

II. THE USE OF THE MURCH SUMMARY WOULD POSE A DIRECT CONFLICT WITH THE JENCKS DECISION.

6. Defendant Scarfo submits that even if the Summary is found to be adequate under CIPA, the use of this summary which admittedly deliberately conceals information (as classified) - which Dr. Farber's affidavit posits is central to the defense - conflicts with the United States Supreme Court decision in Jencks v. United States, 353 U.S. 657, at 670-71, 1 L.Ed.2d 1103, at 1113, 77 S.Ct. 1007 (1957). There, the Court clearly stated:

> But this Court has noticed, in United States v. Reynolds, 345 U.S. 1, the holdings of the Court of Appeals for the Second Circuit that, in criminal causes ". . . the Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also

> has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense. . . ." 345 U.S., at 12.

The Jencks Court cited Learned Hand, often recognized as the tenth Supreme Court Justice:

> In United States v. Andolschek, 142 F.2d 503, 506, Judge Learned Hand said:
>
> '. . . While we must accept it as lawful for a department of the government to suppress documents, even when they will help determine controversies between third persons, we cannot agree that this should include their suppression in a criminal prosecution, founded upon those very dealings to which the documents relate, and whose criminality they will, or may, tend to exculpate. So far as they directly touch the criminal dealings, the prosecution necessarily ends any confidential character the documents may possess; it must be conducted in the open, and will lay bare their subject matter. The government must choose; either it must leave the transactions in the obscurity from which a trial will draw them, or it must expose them fully. Nor does it seem to us possible to draw any line between documents whose contents bears directly upon the criminal transactions, and those which may be only indirectly relevant. Not only would such a distinction be extremely difficult to apply in practice, but the same reasons which forbid suppression in one case forbid it in the other, though not, perhaps, quite so imperatively. . . .' Jencks, supra. at 353 U.S. 671, 1 L.Ed.2d 113.

The Jencks Court held in language that has been adopted by Federal Rules of Criminal Procedure and which has never come close to being overruled:

> We hold that the criminal action must be dismissed when the Government, on the ground of privilege, elects not to comply with an order to produce, for the accused's inspection and for admission in evidence, relevant statements or reports in its possession of government witnesses touching the subject matter of their testimony at the trial. Accord, Roviaro v. United States, 353 U.S. 53, 60-61, 1 L.Ed.2d 639, 644, 645,

> 77 S.Ct. 623. The burden is the Government's, not to be shifted to the trial judge, to decide whether the public prejudice of allowing the crime to go unpunished is greater than that attendant upon the possible disclosure of state secrets and other confidential information in the Government's possession. Jencks, supra. at 353 U.S. 672, 1 L.Ed.2d at 1114.

The government has attempted to withhold information that is absolutely vital to the defense under the guise of complying with CIPA. Compliance with CIPA is not the equivalent of compliance with Jencks.

It is to be remembered that it was the government who injected this highly classified program (KLS) into a domestic bookmaking investigation knowing that what it was doing could pose a threat to national security.

The government cannot bring the prosecution and then dictate the defense. It may not bring the prosecution and at the same time prohibit the defense from properly preparing. It may not bring a prosecution and force the defense to accept its word as final on perhaps the overriding suppression issue.

CIPA envisions the same remedy. CIPA 18 App. Section 6(e)(2).

III. THE MAY AND JUNE, 1999 SEARCH WARRANTS WERE ISSUED AND EXECUTED AS GENERAL WARRANTS.

7. The warrants issued in May and June of 1999 are General Warrants, prohibited by the Fourth Amendment. Since the government admits that its program could distinguish between the various communication ports and ascertain whether or not any were open, it had the ability to capture and record only those keystrokes relevant to the "passphrase." In other words one of the components had the ability to collect only the keystrokes entered when the PGP program was active (Summary paragraphs 9 and 10). If the government wanted to avoid executing a general warrant, it could have easily

limited (or minimized) its information gathering ability to the PGP-only component. By not limiting its information gathering ability to the PGP-only component the government invited, and received, an unnecessary over-collection of data.

Moreover, the Summary admits that every keystroke was "evaluated individually" (Summary pg. 6 paragraph 5 - "... FBI engineers designed this component so that each keystroke was evaluated individually."). Scarfo does not know whether or not these "evaluated" keystrokes were recorded, captured and stored, or were retrievable. To the extent that every keystroke was made available to the government by virtue of the KLS, the warrants as issued and as executed were general warrants.

IV. GIVEN THE FACT THAT THE GOVERNMENT ADMITS THAT IT COULD HAVE LIMITED ITSELF TO THE CAPTURE OR INTERCEPTION OF THE PASSPHRASE ALONE, THERE WAS NO PROBABLE CAUSE FOR THE GOVERNMENT TO SEEK TO CAPTURE OR INTERCEPT KEYSTROKES IN ADDITION TO THE PASSPHRASE.

8. Scarfo submits that the information provided in discovery pertaining to "the data captured from the logger system" is still incomprehensible. While the government's Summary concludes that "the keystroke capture component recorded that the last date when data was actually captured was May 23, 1999," nowhere on the data provided to the defense does a time and or date of capture appear. This data is attached as Exhibit "1".

While there was probable cause to seek to capture and record the passphrase used for the encrypted file, there was no probable cause for the capture and recording of anything other keystrokes. The government admits that its KLS had the surgical ability to limit itself to capturing keystrokes when the encrypted file was activated. Accordingly, the government applied for and secured a general warrant which it executed as a general warrant when it captured and recorded all keystrokes even if such keystrokes were limited to those typed when the communication ports were closed.

Moreover, the data supplied in discovery reflects the capture of both letters, words, numbers, several pages with the word "gray," other indecipherable items and the "passphrase" as its last entry. If the KLS was functioning as it should, this amalgamation of data should not have been recorded - sentences, words, intelligible information should have been recorded. While the government claims that the KLS only operated for 14 days, it is hard to believe that during those 14 days Scarfo hardly wrote an intelligible sentence on his computer.

The dates and times of these captures are essential to Scarfo's defense because the government utilized a device to record the phone numbers called in and out of Scarfo's office during this time (a pen register) and to put the government to the test the defense should be allowed to compare the times Scarfo was online as per the pen register with whatever times the government supplies as to the capture and recording of the KLS.

9. Nor can the government claim that its technology is so sophisticated that it moots the Fourth Amendment. To the government, the greater the technology the less need for Fourth Amendment protection. To Scarfo, the greater the technology the more need for the protection of the Fourth Amendment.

If and when the Court should deliberate on whether the search warrant that issued was a general warrant, Scarfo submits that amongst his other arguments the Court consider that his privacy interests at stake instantly are sheltered by the Fourth Amendment because these privacy interests were precisely those intended to be sheltered by the Framers of our Constitution. The privacy protected by the Fourth Amendment is essentially the entitlement to maintain the confidentiality of information about our lives. Technology clearly threatens this core value when it enables the government to learn facts that could only have been learned through the physical entry and observation by a guard looking over the shoulder of the occupant as he worked at his desk. When the Bill of Rights was adopted this scenario never would have been tolerated. It is intolerable now.

WHEREFORE, it is respectfully requested that this Honorable Court grant Scarfo's Motion to Suppress the seizure of the passphrase and the fruit thereof which is the three Factor files seized on July 15, 1999 which the passphrase opened. In the alternative, it is respectfully requested that this Honorable Court order the government to furnish the defense with the items Dr. Farber delineated in paragraph 17 and in his Conclusion. In the final alternative, if the Court should deny all relief, Defendant Scarfo asks this Court to certify the issues of the adequacy of the Summary under CIPA and the conflict between CIPA and Jencks to the Third Circuit for resolution.

Respectfully submitted,

Vincent C. Scoca, Esquire
Counsel for Nicodemo S. Scarfo
55 Washington Street
Bloomfield, NJ 07003
(973) 680-8949

Norris E. Gelman, Esquire
Co-Counsel for Nicodemo S. Scarfo
The Public Ledger Building
620 Chestnut Street
Suite 940
Philadelphia, PA. 19106
(215) 574-0513

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	CRIMINAL NO. 00-00-404
v.	:	TITLE 18 U.S.C. SECTIONS 894, 1955, and 2
NICODEMO S. SCARFO	:	

DEFENDANT'S MEMORANDUM OF LAW IN SUPPORT OF HIS SUPPLEMENTAL MOTION TO SUPPRESS EVIDENCE SEIZED BY THE GOVERNMENT THROUGH THE USE OF A KEYSTROKE RECORDER

Comes now, Nicodemo S. Scarfo, by and through his legal counsel Vincent Scoca, Esquire and co-counsel Norris E. Gelman, Esquire requesting suppression in accordance with this Motion and a hearing thereon. In support thereof he states:

On October 10, 2001 this Court granted the Government's Motion to Proceed under CIPA and allowed the Government to produce a summary covering the key logger system ("KLS") in question. The Court later found this Summary to be adequate under CIPA so as to allow further proceedings.

I. THE RANDALL S. MURCH SUMMARY IS NOT ADEQUATE UNDER CIPA.

The Summary does not comply with CIPA Section 6(c)(1) because it fails to "provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information."

Dr. Farber in his affidavit states that the Summary 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 vagueness and its lack of an adequate foundation on which to base the conclusions it forwards. (See attached Affidavit from Dr. David Farber which is Exhibit "1"). As a result, this Court still cannot determine whether or not the KLS intercepted or captured electronic communications implicating Title III.

Not only does the Summary fail to meet the standards of the scientific community from which it purports to emanate because of its vagueness and its delivery of raw conclusions without a supporting factual basis. In other words, the Summary as expert testimony, would not even be admissible in Court. Any expert who would insist on informing the Court of his or her conclusions but not the underlying basis for such conclusions would see his or her testimony stricken from the record.

The defense should not be saddled with such a Summary and told that it is close enough for government work.

II. THE USE OF THIS SUMMARY CONFLICTS WITH THE JENCKS DECISION

Defendant Scarfo submits that even if the Summary is found to be adequate under CIPA, the use of this summary which admittedly deliberately conceals information (as classified) - which Dr. Farber's affidavit posits is central to the defense - conflicts with the United States Supreme Court decision in Jencks v. United States, 353 U.S. 657, at 670-71, 1 L.Ed.2d 1103, at 1113, 77 S.Ct. 1007 (1957). There, the Court clearly stated:

> But this Court has noticed, in United States v. Reynolds, 345 U.S. 1, the holdings of the Court of Appeals for the Second Circuit that, in criminal causes ". . . the Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal

> cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense. . . ." 345 U.S., at 12 (Emphasis supplied)

The Jencks Court held in language that has been adopted by Federal Rules of Criminal Procedure and which has never come close to being overruled:

> We hold that the criminal action must be dismissed when the Government, on the ground of privilege, elects not to comply with an order to produce, for the accused's inspection and for admission in evidence, relevant statements or reports in its possession of government witnesses touching the subject matter of their testimony at the trial. Accord, Roviaro v. United States, 353 U.S. 53, 60-61, 1 L.Ed.2d 639, 644, 645, 77 S.Ct. 623. The burden is the Government's, not to be shifted to the trial judge, to decide whether the public prejudice of allowing the crime to go unpunished is greater than that attendant upon the possible disclosure of state secrets and other confidential information in the Government's possession. Jencks, supra. at 353 U.S. 672, 1 L.Ed.2d at 1114.

The government has attempted to withhold information that is absolutely vital to the defense under the guise of complying with CIPA. Compliance with CIPA is not the equivalent of compliance with Jencks.

It is to be remembered that it was the government who injected this highly classified program (KLS) into a domestic bookmaking investigation knowing that what it was doing could pose a threat to national security.

The government cannot bring the prosecution and then dictate the defense. It may not bring the prosecution and at the same time prohibit the defense from properly preparing. It may not bring a prosecution and force the defense to accept its word as final on perhaps the overriding suppression issue. The defense has the right to review the data to see if it can be used to benefit the defense - especially when it is as incredibly relevant as in the instant case.

The defense should not be forced to accept that data as screened by the government.

III. THE WARRANT REQUESTED AND EXECUTED WAS A GENERAL WARRANT

Scarfo perceives a vast difference between what the government says its KLS did and what it recorded. The government asserts that its KLS would not capture and record any electronic communication - but was limited by its operation to capturing and recording key strokes when all communication portals were closed. The government has turned over what its KLS did capture and record and it is attached hereto as Exhibit "2". One would expect that the data secured by the government would be what anyone else would type on a computer over a 14 day period - not the hundreds of "gray" and other incomprehensible data the government provided. Yet, amongst this data one can find phone numbers, partial sentences about jewelry, references to mom and grand pop about reading glasses, and a few other partial phrases or sentences.

While the government insists it secured the passphrase on or before May 23, 1999 there is no way Scarfo can read this date on the information he was given in discovery.

The government admitted that it had the technology to seek only the passphrase and as stated in the attached Motion, to purposely secure information over and above the passphrase is to turn the search into a general one.

Moreover, while the government did have probable cause to believe that the passphrase could be secured from the computer in question, it did not have probable cause to collect all of Scarfo's keystrokes - even if they were collected when all communication ports were closed. The taint of the excessive exploration or general search converts what should have been a limited search for a passphrase into a

general warrant and a general search which should be suppressed. The government cannot be heard to argue that it acted in good faith in securing such a warrant.

WHEREFORE, it is respectfully requested that this Honorable Court grant Scarfo's Motion to Suppress the seizure of the passphrase and the fruit thereof which is the three Factor files seized on July 15, 1999 which the passphrase opened. In the alternative, it is respectfully requested that this Honorable Court order the government to furnish the defense with the items Dr. Farber delineated in paragraph 17 and in his Conclusion. In the final alternative, if the Court should deny all relief, Defendant Scarfo asks this Court to certify the issues of the adequacy of the Summary under CIPA and the conflict between CIPA and Jencks to the Third Circuit for resolution.

Respectfully submitted,

Vincent C. Scoca, Esquire
Counsel for Nicodemo S. Scarfo
55 Washington Street
Bloomfield, NJ 07003
(973) 680-8949

Norris E. Gelman, Esquire
Co-Counsel for Nicodemo S. Scarfo
The Public Ledger Building
620 Chestnut Street
Suite 940
Philadelphia, PA. 19106

(215) 574-0513

EXHIBIT 1

Note: digital version does not include Dr. Farber’s CV

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	CRIMINAL NO. 00-00-404
	:	
V.	:	HON. NICOLAS H. POLITAN, U.S.D.J.
	:	
NICODEMO S. SCARFO	:	

AFFIDAVIT OF DAVID J. FARBER

I, DAVID J. FARBER, being duly sworn do hereby state and aver:

1. I am the Alfred Fitler Moore Professor of Telecommunication Systems at the University of Pennsylvania, holding appointments in the Departments of Computer Science and Electrical Engineering.
2. During my career, as detailed in my curriculum vitae, I served as Chief Technologist at the FCC, until January of 2001. I served three years on the Presidential Advisory Committee on Information Technology.
3. I have received in the past TOP SECRET clearance at the RAND Corporation and SECRET for the National Research Council/
4. I have reviewed the summary prepared by Randall S. Murch, Deputy Assistant Director at the FBI concerning the Key Logger System ("KLS").
5. This summary is inadequate for me, or for anyone knowledgeable in the computer field, to be able to ascertain with the requisite degree of scientific certainty that the KLS did not intercept or capture electronic communications (email, instant messaging, etc.). In other words, while this summary does purport to conclude that the KLS did not engage in any such capture, such a conclusion or conclusions cannot

be drawn from it because of its vagueness and its lack of any foundation on which to build such a conclusion or conclusions.

6. If I were called to testify in this case, testimony would be based upon my lifetime of experience in the field of computer science and telecommunications. I believe that my opinions represent commonly understood and accepted principles and practices in the field of computer science which are applicable to all software, hardware and or firmware, whether developed by the government or any other entity.
7. Disclosure of the information requested herein will not reveal source code or other information, which could jeopardize national security.
8. The summary of Randall S. Murch (hereafter "summary") describes several procedures that are performed by the KLS (for example, evaluating the key stroke, checking communication ports, checking the active windows). There is no explanation of how these procedures relate to each other and support the allegation that the KLS did not capture online communication or every keystroke. Further it is impossible to determine if there were any safeguards in the event of a malfunction of one or more of the procedures.
9. Paragraph 5 of the summary indicates that an examination of the targeted computer was made. In order to determine whether the KLS operated as claimed, I need to review the actual summary made by the Government, as well as the procedures, software utilities and the actual targeted computer. This is particularly necessary because by the Government's own assertion, the computer was at various times inoperable. Its specific configuration is essential in order to evaluate whether or not the KLS could have worked as claimed on this particular computer. Also, it is

necessary to determine if one of a commonly available counter measures was present which would disable the system if a foreign agent (program or device) had been installed on it. For example, many anti-virus programs will disable an entire system and quarantine the foreign program (virus). Other devices, which are readily available, such as Spycop (http://spycop.com/), detect key logger devices and foreign surveillance agents and take corrective action. It is important to know whether these types of applications were present and if so, how the Government's KLS dealt with them.

10. There are many aspects of the summary that are contradictory. In paragraph 5 of the summary it claims, "Further, the FBI did not install and operate any KLS component which would search for or record any fixed data stored within the computer." If this were true, then how would the agents retrieve the actual recorded keystrokes from the system? Unless another program was used. This would be another piece of this technical puzzle that must be given in order to properly evaluate the function of the device.

11. Paragraph 6 of the summary makes reference to the targeted computer being evaluated. It states that the computer had no other means of external communication, other than the modem connected to a communication port. Without inspecting the targeted computer there is no way to determine whether or not there was another communication device installed, such as a network card, prior to, during or after the installation and operation of the KLS.

12. Paragraph 7 of the summary asserts that in a Microsoft Windows ® environment, a word processing program is incapable of utilizing online communications. In fact,

Microsoft Outlook ® (which is bundled with the Microsoft Office ® Suite of programs) has the option of using Microsoft Word ® as its primary email editor.

> *In order to access this option one must load MS Outlook and choose "Tools" on the menu bar, then chose "Options" then chose "Mail Format" then check "Use Microsoft Word to edit email messages".*

The Microsoft Windows® operating system is integrated so that all parts of the system can utilize and be utilized by a remote location. This may be accomplished by either a modem or a network card.

13. Also, in paragraph 7 of the summary, asserts that while a modem is connected to the Internet Service Provider (ISP, AOL in this case) that it does not necessarily have to be engaged in sending electronic communications. When a subscriber is online and connected via their ISP, communications constantly go back and forth between the subscriber's computer and the service. If the summary was accurate in asserting the contrary, neither the ISP nor the subscriber would know the connection was still active

14. In paragraph 8 of the summary, it mentions that the program PGP was not configured to communicate online. Without my evaluation of the configuration of the target computer and the particular version of PGP, as configured on that computer, it is impossible conclude that PGP did not act online or that it was not used for electronic communications.

15. I have been advised by counsel that during the period of the operation of the KLS the target computer was experiencing persistent technical malfunction. This was also noted in paragraph 13 of the summary. Specifically, I was told that the "6" key on the

number pad was not operating and that the system would not "boot-up" properly. With these types of errors occurring in any non-healthy system I am concerned that;

a. The KLS was the cause of the malfunctions, and/or

b. The operations of KLS could have been affected by the malfunctions causing the KLS or any of its parts to not operate as designed.

16. The summary states that multiple points of surveillance and evaluations were performed with each keystroke. There was and is the technology that the government possessed that would have allowed them to accomplish their goals in a much more simplified manner. The government knew that AOL (America Online) was the service used for the targeted computer. They also knew that AOL's primary function is for online communication. They had software installed on the targeted computer that knew when certain programs were loaded such as PGP, AOL or a word processor. When all that was needed to perform the government's goal was to install software that only loaded when PGP was loaded and not record a single keystroke when AOL was loaded. They could have used the same software (as described in their summary) that was installed on the targeted computer. There was no need to evaluate every single keystroke that was made.

17. In order to form an adequate opinion of the KLS, its operations, its installation, the stability of the targeted computer and any software, hardware and or firmware that was used to evaluate, remove or maintain the recorded keystrokes. I would need the following;

a. A copy of any data that was removed from the targeted computer including

i. Mirror images of the hard drive before, during and after the KLS was present.

ii. The specifications of any additional software, hardware and/or firmware that was used to evaluate, remove and/or analyze data from the targeted computer.

iii. A copy of the data that was captured by the KLS from the targeted computer, in its digital form.

By disclosing the raw data (electronic format) of the information captured by the KLS, there will be no disclosure of any of the intricacies of the operation of the KLS. This data is critical in determining if the KLS operated as claimed.

iv. The actual "targeted" computer that the government installed the KLS on.

CONCLUSION

The summary provided by Randall S. Murch is insufficient because it is written in such a manner that it is capable of various meanings, which can only be clarified by an explanation of the operation of the key logger. While this vagueness may be necessitated by the fact that much of the information being summarized is classified, it also prevents the defense from receiving a summary that is sufficient to dispel the defense fears that electronic communications were captured in the operation of the KLS. The summary also fails to adequately explain what triggers or actuates the recording of the keystrokes.

Finally, the summary is inadequate because it would not pass muster in the scientific community as being a valid summary of what has transpired here. Its vagueness alone would cause it to be rejected as either a valid or as a useful summary by experts in the field.

In any technical field, the delivery of raw conclusions without first providing the factual basis for those conclusions is unacceptable.

The summary raises more questions than it answers. And, any answer (conclusion) that it does provide is one, which is totally dependent on the credibility and integrity of its author. While the author may be entirely correct in his raw assertions, the scientific method cautions, indeed sets its face against, such blind acceptance.

_____

David J. Farber

Sworn to and subscribed before me this _____ day of November 2001

_____

Notary Public

EXHIBIT 2

Note: Digital version does not include this Exhibit