

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA)

v.)

NICODEMO S. SCARFO, and)
FRANK PAOLERCIO)

Criminal No. 00-404

HON. NICOLAS H. POLITAN, U.S.D.J.

AFFIDAVIT OF RANDALL S. MURCH

I, Randall S. Murch, Laboratory Division, Federal Bureau of Investigation, hereby declare, under penalty of perjury, the following:

AFFIANT.

- I. I am a Supervisory Special Agent of the Federal Bureau of Investigation (FBI), currently assigned to the FBI's Laboratory Division as a Deputy Assistant Director and have been an employee of the FBI for over 21 years. My prior relevant assignments in the FBI include the Special Projects Technologies Section of the National Security Division, an assignment to the Investigative Technologies Branch as the Unit Chief of the Advance Technologies and Applications Unit, as well as a technical management assignment in the New York Division's Special Operations Division. Further, I previously served as the Section Chief (department head) and the Deputy Assistant Director (head) of the Laboratory Division's Forensic Analysis Branch, which included technical aspects of National Security and Counter Terrorism/Counter Intelligence Research and

Development. I was also detailed to the Department of Defense's Defense Threat Reduction Agency for the development of advanced concepts in technology, policy, and operational concepts in National Security. I have been awarded a Ph. D. in Life Sciences, and have extensive engineering experience. I am currently the Deputy Assistant Director of the FBI Laboratory Division's Investigative Technologies Branch. As part of my responsibilities, I am responsible for many of the programs which support the FBI's electronic surveillance and technical search and seizure capabilities. As such, I am familiar with the various technological endeavors, equipment, and systems which the FBI deploys in both criminal investigations and national security cases and am periodically briefed and advised on such equipment and systems by subordinates. In this regard, I am familiar with the technology that was used by the FBI to capture the key and key-related information in support of the investigation of Nicodemo S. Scarfo (hereinafter the "key logger system"¹ (KLS)). It is based upon that collective and specific knowledge, information and belief, which I, in fact, believe to be true, that I submit this affidavit.

BACKGROUND OF CASE

Nature of PGP

2. PGP is a commercially available encryption program, and in fact is

¹ As used throughout this affidavit, the term "key," when used alone without modifiers refers to one or more "encryption key(s)." The term "keystroke" refers to the selection by a user of a keyboard key.

available free via the Internet to individual users. Upon installation on a computer, this program can be configured to use different encryption algorithms, such as DES (Data Encryption Standard), Triple DES and IDEA: A person using PGP encryption may encrypt (e.g., encipher or encode) the plain text of his/her files, store those files, and decrypt them. In this way, the PGP user prevents anyone not possessing the appropriate encryption key and key-related information² from decrypting (e.g., deciphering or decoding) the files.

3. A user of the PGP program normally creates one "public and private key pair" (i.e., the keys are associated with each other) for himself. A user's public key is used in the process of encrypting data such that only the user can decrypt that data using the paired "private key." In addition to encrypting files intended to merely be stored on a user's computer, a PGP user, in conjunction with other PGP users, may use PGP to securely encrypt incoming or outgoing files and/or message files. The user may share his public key with others who may then send that user files and/or message files which have been securely encrypted by the sender utilizing the intended recipient's (the user's) public key. Public and private PGP keys tend to be long strings of computer data typically not capable of being memorized by users. As a result, a simpler passphrase is used to protect the private key. A "session key" is randomly generated by the PGP program each time a file is encrypted. In reality, files are actually encrypted with the session

² Key and key-related information refers to passphrases, passwords, encryption keys as well as other technical aspects of the PGP process itself being utilized in a particular instance.

key, and the session key is then, in turn, encrypted with the recipient's public key. In order to decrypt a file encrypted with a user's public key, the PGP software program calls up a specific and known PGP computer file which displays to the computer screen (via a graphics/video card in the computer) a specific and known graphics user interface "dialog" box. This dialog box acts to visually prompt the user decrypting the file to enter, via the keyboard, the "passphrase" associated with the appropriate "private key." When the user enters the proper passphrase, PGP verifies that the passphrase is correct and if so, uses that passphrase to decrypt the private key. This private key is then used to decrypt that session key, which is, in turn, used to decrypt the selected file. Therefore, in order to decrypt a PGP encrypted file it is necessary to have the encrypted file, the appropriate private key, the passphrase associated with this private key, and the PGP program.

THE KEY LOGGER SYSTEM (KLS)

Background

4. In this case, the Newark FBI office requested FBI Laboratory assistance in acquiring Scarfo's key and key-related information. In response, FBI engineers configured a hardware/software and/or firmware solution based upon previously developed techniques which would permit the FBI to obtain the defendant's key and key-related information. These techniques, and their various components, have come to be known collectively within the FBI as the Key Logger System (KLS). The KLS was devised by the FBI, and is exclusively the property of the

FBI. The KLS, depending upon the hardware and software configuration of a targeted computer and the use of that computer, can, and typically will, have multiple components.

5. Examination and evaluation of Scarfo's stand alone computer by the FBI during and subsequent to the entry authorized by the order of January 15, 1999, revealed that the system had generally four mechanisms or domains through which key or key-related information could possibly enter or exit the encryption/decryption processes: (1) from a transmission pathway through a modem attached to the computer; (2) by retrieval from storage; (3) by entry by someone typing on the keyboard; and (4) by the computer itself by one or more processes working within that computer. The challenge for the FBI in this situation was to devise a technical search capability which could search for and record key or key-related information entered through at least one of these mechanisms without detection and without either searching or seizing any information which, in addition to being key or key-related information, could also be an electronic communication. The FBI, as a part of the KLS deployed in the instant investigation, did not install and operate any component which would search for and record data entering or exiting the computer from the transmission pathway through the modem attached to the computer. Further, the FBI did not install and operate any KLS component which would search for or record any fixed data stored within the computer.
6. A component of the KLS deployed in this case was a "keystroke capture"

component that was designed to record, under certain conditions described below, each keystroke typed on a keyboard. This component was imbedded into Scarfo's computer in such a way as to conceal its very existence amidst other pre-existing elements of the computer. As indicated above, during the initial examination of the defendant's computer and hard drive during the entry authorized by the order of January 15, 1999, the FBI noted that the defendant had a modem installed and connected to his computer. The FBI recognized that during those times when the defendant or any other user activated the modem, the computer would be capable of transmitting electronic communications via the modem. Conversely, however, because that examination of Scarfo's computer revealed that it possessed no other common or recognizable means of communicating with other computers except through the modem, the FBI knew that when the computer's modem was not activated, the computer was not acting as an electronic communications device. The FBI's examination of this computer revealed that it utilized a modem connected to a communication port. In order to avoid potentially intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports, FBI engineers designed this component so that each keystroke was evaluated individually. The default status of the keystroke component was set so that, on entry, a keystroke was normally not recorded. Upon entry or selection of a keyboard key by a user, the KLS checked the status of each communication port installed on the computer, and, all communication ports indicated inactivity,

meaning that the modem was not using any port at that time, then the keystroke in question would be recorded.

7. As described above, the Key Logger System may be made up of multiple components depending on the configuration of the computer system authorized for search. In this case, another component or components of the KLS worked to complement the first component to address potential passphrase collection shortfalls that might occur in the keystroke capture components of the KLS. For example, if Scarfo was online, the modem would be on and the keystroke capture component would, by default, not record keystrokes. However, the fact that the modem of a computer is active, does not necessarily mean that the computer is, at that moment, engaged in sending electronic communications. In fact, in a Microsoft Windows ® operating system environment (which was the operating system on Scarfo's computer), a computer user can activate the computer's modem in one "window" in relationship to one application (e.g., AOL), then open and switch to a second "window" and actively work in that second window in an application incapable of engaging in electronic communications (e.g., a word processing program), but capable of executing the PGP program. Thus, if Scarfo was simultaneously working in a separate window using his PGP program to decrypt files, the keystroke capture component would not have captured and recorded his keystrokes and, hence, would not have captured a PGP passphrase.

8. Examination of the defendant's computer by agents of the FBI during entries authorized by court order revealed that the PGP program as configured on

his computer and as used by the defendant during all relevant time periods was not technically capable of sending his passphrase over a network in any way. This meant that all of the PGP program's functions and operations originated from the computer's hard drive, with the exception of the passphrase which was entered by the defendant via the keyboard. This also meant that all actions involving either encryption or decryption necessarily occurred only within his computer, and not on some other networked computer connected via modem. This would be true even if Scarfo was using PGP on his computer and the modem was coincidentally activated (e.g., being used by another computer program such as AOL in another "window").

9. As indicated above, the PGP software program visually prompts (via a display on the computer screen) the user who is decrypting a file for the "passphrase" associated with the appropriate "private key." The passphrase itself is typed via keystrokes on the keyboard and then entered into the PGP program when the user hits/selects the "enter" or "return" key at the conclusion of the passphrase. When the user enters the proper passphrase, PGP verifies that the passphrase is correct and if so, uses that passphrase to decrypt the private key.

10. The FBI developed a mechanism to record the passphrase as entered via the keyboard by the user and certain other key-related information. The FBI recognized that it was possible for the defendant to use PGP in sequential combination with wide array 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 passphrase 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 without impairing functionality or jeopardizing the covert operation of the KLS. Accordingly, the multiple components of the KLS complemented each other, while operating within the parameters of the court's orders specifying that the KLS would not capture communications subject to Title III.

RESULTS OF KLS

Disclosure of Output

11. As described above, there can be a number of varying, but interrelated components to the KLS depending upon the configuration and use of the computer authorized for search. Generally speaking, each component is capable of producing output. The outputs are surreptitiously recorded and can be recorded separately.
12. A pen register analysis for the telephone numbers at the computer's location revealed, and as the defendant has acknowledged in a prior pleading, during the first 10 days of the 60 day period of authorized monitoring, the defendant appears to have networked to AOL more than 30 times. As noted, the keystroke capture component was specifically designed so that capturing and recording data during any time the modem was in actual operation was not

possible. Therefore, it logically follows that there would be no data recorded by the keystroke capture component for each time period in which the defendant was connected to a computer network through his modem. To comply with discovery in this case, all portions of the KLS which did in fact produce outputs, drawn from the multiple components installed, were combined into one document, presented and transmitted as the total output of the Key Logger System. (July 17, 2001 Brief in Opposition to Defendant Scarfo's Pretrial Motion, Exh. D). Other than the output that was captured by the keystroke component, as described above, 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.

Recovery of Output

13. In order to recover the output of the KLS, it was necessary to gain physical access to the computer. A total of five surreptitious entries into Scarfo's place of business were made. On four of those occasions, the computer in question was found to be inoperative or not present. On only one of those occasions was the computer in question found to be present and in working order.

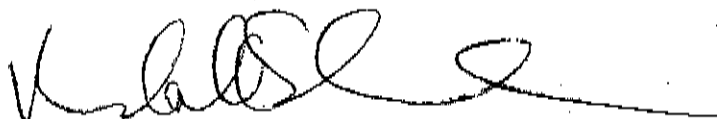
Volume of Output

14. In addition, the keystroke capture component recorded that the last date when data was actually captured was May 23, 1999. This was a mere 14 days following the installation. Therefore, the total amount of time that the FBI actually collected keystrokes from the defendant's computer was only 14 days,

rather than the 60 days authorized in the Court's two orders.

15. In conclusion, the KLS, by design, prohibited the capture of keyboard keystrokes whenever the computer modem was on; other component(s), described above, limited their capture to only the passphrase and key-related information. Given the fact that Scarfo's computer was present and in working order on only one of the five authorized surreptitious entries, the volume of the output from the FBI's KLS is entirely consistent with the use of the defendant's computer.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on this 4th day of October, 2001.



Randall S. Murch
Deputy Assistant Director
Investigative Technology Branch,
FBI Laboratory Division