Re: United States v. Nicodemo S. Scarfo, et al.

Criminal Action No. 00-404 (NHP)

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY

180 F. Supp. 2d 572*; *2001 U.S. Dist. LEXIS 21561

December 26, 2001, Decided

JUDGES: NICHOLAS H. POLITAN, U.S.D.J.

OPINION BY: NICHOLAS H. POLITAN

OPINION

Dear Counsel:

This matter comes before the Court on Defendant Nicodemo S. Scarfo's ("Scarfo") pretrial motion for discovery and suppression of evidence. The Court heard oral argument on July 30, 2001 and again on September 7, 2001. Co-defendant Frank Paolercio ("Paolercio") joined in the motion. The government thereafter moved to invoke the Classified Information Procedures Act. For the following reasons, the Defendants' motion for **[**2]** discovery is granted in part and denied in part, and the motion to suppress evidence is denied.

BACKGROUND

This case presents an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity. It appears that no district court in the country has addressed a similar issue. Of course, the matter takes on added importance in light of recent events and potential national security implications.

The Court shall briefly recite the facts and procedural history of the case. Acting pursuant to federal search warrants, the F.B.I. on January 15, 1999, entered Scarfo and Paolercio's business office, Merchant Services of Essex County, to search for evidence of an illegal gambling and loansharking operation. During their search of Merchant Services, the F.B.I. came across a personal computer and attempted to access its various files. They were unable to gain entry to an encrypted file named "Factors."

Suspecting the "Factors" file contained evidence of an illegal gambling and loansharking operation, the F.B.I. returned to the **[**3]** location and, pursuant to two search warrants, installed what is known as a "Key Logger System" ("KLS") on the computer and/or computer keyboard in

order to decipher the passphrase to the encrypted file, thereby gaining entry to the file. The KLS records the keystrokes an individual enters on a personal computer's keyboard. The government utilized the KLS in order to "catch" Scarfo's passphrases to the encrypted file while he was entering them onto his keyboard. Scarfo's personal computer features a modem for communication over telephone lines and he possesses an America Online account. The F.B.I. obtained the passphrase to the "Factors" file and retrieved what is alleged to be incriminating evidence.

On June 21, 2000, a federal grand jury returned a three-count indictment against the Defendants charging them with gambling and loansharking. The Defendant Scarfo then filed his motion for discovery and to suppress the evidence recovered from his computer. After oral argument was heard on July 30, 2001, the Court ordered additional briefing by the parties. **[*575]** In an August 7, 2001, Letter Opinion and Order, this Court expressed serious concerns over whether the government violated the wiretap **[**4]** statute in utilizing the KLS on Scarfo's computer. Specifically, the Court expressed concern over whether the KLS may have operated during periods when Scarfo (or any other user of his personal computer) was communicating via modem over telephone lines, thereby unlawfully intercepting wire communications without having applied for a wiretap pursuant to Title III, *18 U.S.C. § 2510*. . . .

DISCUSSION

I. General Warrant

Scarfo argues that since the government had the ability to capture and record only those keystrokes relevant to the "passphrase" to the encrypted file, and because it received an unnecessary over-collection of data, the warrants were written and executed as general warrants. This claim is without merit.

Typically, the proponent of a motion to suppress bears **[**9]** the burden of establishing that his *Fourth Amendment* rights were violated. See *United States v. Acosta, 965 F.2d 1248, 1257 n.9 (3d Cir. 1992)* (citing *Rakas v. Illinois, 439 U.S. 128, 130 n.1, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1979)*). The standard of proof in this regard is a preponderance of the evidence. See *United States v. Matlock, 415 U.S. 164, 178 n.14, 94 S. Ct. 988, 39 L. Ed. 2d 242 (1974)* ("The controlling burden of proof at suppression hearings should impose no greater burden than proof by a preponderance of the evidence.").

It is settled that at a hearing on a motion to suppress, "the credibility of the witnesses and the weight to be given the evidence, together with the inferences, deductions and conclusions to be drawn from the evidence, are all matters to be determined by the trial judge." *United States v. McKneely, 6 F.3d 1447, 1452-53 (10th Cir. 1993)*. See also *United States v. Matthews, 32 F.3d 294, 298 (7th Cir. 1994)*; *United States v. Cardona-Rivera, 904 F.2d 1149, 1152 (7th Cir. 1990)*; *Government of the Virgin Islands v. Gereau, 502 F.2d 914, 921* **[*577]** *(3d Cir. 1974)*, **[**10]** cert. denied, *420 U.S. 909, 95 S. Ct. 829, 42 L. Ed. 2d 839 (1975)*.

The *Fourth Amendment* states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *U.S. CONST. amend. IV*. Where a search warrant is obtained, the

Fourth Amendment requires a certain modicum of particularity in the language of the warrant with respect to the area and items to be searched and/or seized. See *Torres v. McLaughlin, 163 F.3d 169, 173 (3d Cir. 1998)*, cert. denied, *528 U.S. 1079, 120 S. Ct. 797, 145 L. Ed. 2d 672 (2000)*. The particularity requirement exists so that law enforcement officers are constrained from undertaking a boundless and exploratory rummaging through one's personal property. See *United States v. Johnson, 690 F.2d 60, 64 (3d Cir. 1982)* (citing *Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971))*, cert. denied, *459 U.S. 1214, 103 S. Ct. 1212, 75 L. Ed. 2d 450 (1983)*.

From a review of the two Court Orders authorizing the searches **[**11]** along with the accompanying Affidavits, it is clear that the Court Orders suffer from no constitutional infirmity with respect to particularity. Magistrate Judge Donald Haneke's May 8, 1999, Order permitting the search of Scarfo's computer clearly states that Judge Haneke found probable cause existed to believe that "Nicodemo S. Scarfo has committed and continues to commit offenses in violation of Title *18, U.S.C. §§ 371*, 892-94, *1955* and *§ 1962*." See Judge Haneke's May 8, 1999 Order, at P 1. That Order further stated that there was "probable cause to believe that Nicodemo S. Scarfo's computer, located in the TARGET LOCATION, is being used to store business records of Scarfo's illegal gambling business and loansharking operation, and that the above mentioned records have been encrypted." See Judge Haneke's May 8, 1999 Order, at P 3.

Because the encrypted file could not be accessed via traditional investigative means, Judge Haneke's Order permitted law enforcement officers 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 **[**12]** the F.B.I. can capture the password necessary to decrypt computer files by recording the key related information as they are entered." See Judge Haneke's May 8, 1999 Order, at pp. 4. The Order also allowed the F.B.I. to

> search for and seize business records in whatever form they are kept (e.g., written, mechanically or computer maintained and any necessary computer hardware, including computers, computer hard drives, floppy disks or other storage disks or tapes as necessary to access such information, as well as, seizing the mirror hard drive to preserve configuration files, public keys, private keys, and other information that may be of assistance in interpreting the password)-- including address and telephone books and electronic storage devices; ledgers and other accounting-type records; banking records and statements; travel records; correspondence; memoranda; notes; calendars; and diaries-- that contain information about the identities and whereabouts of conspirators, betting customers and victim debtors, and/or that otherwise reveal the origin, receipt, concealment or distribution of criminal proceeds relating to illegal gambling, loansharking and other racketeering **[**13]** offenses.

See Judge Haneke's May 8, 1999 Order, at pp. 4-5.

[*578] On its face, the Order is very comprehensive and lists the items, including the evidence in the encrypted file, to be seized with more than sufficient specificity. See *Andresen v. Maryland, 427 U.S. 463, 480-81, 96 S. Ct. 2737, 2748-49, 49 L. Ed. 2d 627 (1976)* (defendant's

general warrant claim rejected where search warrant contained, among other things, a lengthy list of specified and particular items to be seized). One would be hard-pressed to draft a more specified or detailed search warrant than the May 8, 1999 Order. Indeed, it could not be written with more particularity. It specifically identifies each piece of evidence the F.B.I. sought which would be linked to the particular crimes the F.B.I. had probable cause to believe were committed. Most importantly, Judge Haneke's Order clearly specifies the key piece of the puzzle the F.B.I. sought - Scarfo's passphrase to the encrypted file.

That the KLS certainly recorded keystrokes typed into Scarfo's keyboard other than the searched-for passphrase is of no consequence. This does not, as Scarfo argues, convert the limited search for the passphrase into a general exploratory search. During many lawful searches, police officers may not know the exact nature of the incriminating evidence sought until they stumble upon it. Just like searches for incriminating documents in a closet or filing cabinet, it is true that during a search for a passphrase "some innocuous [items] will be at least cursorily perused in order to determine whether they are among those [items] to be seized." *United States v. Conley, 4 F.3d 1200, 1208 (3d Cir. 1993)*. See also *United States v. Carmany, 901 F.2d 76 (7th Cir. 1990)* (upholding seizure of unregistered handgun found in filing cabinet while validly executing warrant to discover evidence relating to cocaine distribution charges) *United States v. Fawole, 785 F.2d 1141, 1145 (4th Cir. 1986)*; *United States v. Santarelli, 778 F.2d 609, 615-16 (11th Cir. 1985)* (search warrant entitled agents to search for documents, i.e., **[**15]** records of loansharking activity, etc., and agents were entitled to examine each document in bedroom or in filing cabinet to determine whether it constituted evidence they were entitled to seize under warrant); *United States v. Issacs, 708 F.2d 1365, 1368-70* (9th Cir.), cert. denied, *464 U.S. 852, 104 S. Ct. 165, 78 L. Ed. 2d 150 (1983)*; *United States v. Christine, 687 F.2d 749, 760 (3d Cir. 1982)*.

Hence, "no tenet of the *Fourth Amendment* prohibits a search merely because it cannot be performed with surgical precision." *Conley, 4 F.3d at 1208* (quoting *United States v. Christine, 687 F.2d 749, 760 (3d Cir. 1982))*. Where proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant. As the Supreme Court stated in Andresen, "the complexity of an illegal scheme may not be used as a shield to avoid detection when the [government] has demonstrated **[**16]** probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession." *Andresen, 427 U.S. at 482, 96 S. Ct. at 2749 n.10*. Accordingly, Scarfo's claim that the warrants were written and executed as general warrants is rejected. . . .

IV. Whether the KLS Intercepted Wire Communications

The principal mystery surrounding this case was whether the KLS intercepted a wire communication in violation of the wiretap statute by recording keystrokes of e-mail or other communications made over a telephone or cable line while the modem operated. These are the only conceivable wire communications which might emanate from Scarfo's computer and potentially fall under the wiretap statute.

Upon a careful and thorough review of the classified information provided to the Court on September 26th and the Murch Affidavit, the Court finds that the **[**24]** KLS technique utilized in deciphering the passphrase to Scarfo's encrypted file did not intercept any wire communications and therefore did not violate the wiretap statute, Title III, *18 U.S.C. § 2510*. I am satisfied the KLS did not operate during any period of time in which the computer's modem was activated.

Scarfo's computer contained an encryption program called PGP (Pretty Good Privacy), which is used to encrypt or scramble computer files so that decrypting or unscrambling the files requires use of the appropriate passphrase. According to the Murch Affidavit, in order to decrypt an encrypted file, the PGP software displays on the user's computer screen a "dialog box." See Murch Aff., P 3. The user then must enter, via the keyboard, the "passphrase" into the dialog box. See id. When the proper passphrase is entered, PGP verifies that the passphrase is correct and, after several steps, leads to the decryption of the selected file. See id.

The KLS, which is the exclusive property of the F.B.I., was devised by F.B.I. engineers using previously developed techniques in order to obtain a target's key and key-related information. See Murch Aff. **[**25]** , P 4. As part of the investigation into Scarfo's computer, the F.B.I. "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." Murch Aff., P 5. Neither did the F.B.I. "install or operate any KLS component which would search for or record any fixed data stored within the computer." See id.

Recognizing that Scarfo's computer had a modem and thus was capable of transmitting electronic communications via the modem, the F.B.I. configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously **[*582]** transmitted in real time via the communication ports. See Murch Aff., P 6. To do this, the F.B.I. designed the component "so that each keystroke was evaluated individually." See id. As Mr. Murch explained:

> 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 **[**26]** that the modem was not using any port at that time, then the keystroke in question would be recorded.

Hence, when the modem was operating, the KLS did not record keystrokes. It was designed to prohibit the capture of keyboard keystrokes whenever the modem operated. See Murch Aff., P 15. Since Scarfo's computer possessed no other means of communicating with another computer save for the modem, see Murch Aff., P 6, the KLS did not intercept any wire communications. [5] Accordingly, the Defendants' motion to suppress evidence for violation of Title III is denied.

5 In addition, since all of the PGP program's functions and operations originated from the computer's hard drive, all actions involving either encryption or decryption occurred only within Scarfo's computer, and not on some other networked computer connected via modem. See Murch Aff., P 8.