CRACKING THE CODE TO PRIVACY: HOW FAR CAN THE FBI GO?

As the Nation continues to deal with the fallout of the events of September 11th, it must continue to decide what limits on privacy will be sacrificed in order to allow the government to tighten its security efforts. Who would have guessed that in this crazy post-September 11th world, the latest champion of Constitutional freedoms would be a reputed mobster?

Introduction

That is exactly what is happening in New Jersey, where Nicodemo Scarfo, Jr., on trial for gambling and loan-sharking, is taking on the FBI, claiming that the search tactics used violated his Fourth Amendment rights. FBI agents used a device known as a Key Logger System ("KLS") to record the keystrokes typed on Scarfo's computer keyboard, and thus obtained the password needed to break through his encryption software and open a file. On December 26, 2001, the district court judge ruled on two pre-trial motions, holding that the FBI's use of a KLS was lawful. The judge further held that Scarfo was not entitled to detailed information about the KLS system because its classified nature would present a credible threat to national security if it were revealed, especially in light of the recent terrorist attacks. This case is the first of its kind, and the potential implications for criminal investigations are sobering.

Previous FBI computer technology such as the Carnivore system is deployed online and does not require the physical installation of anything onto a suspect's computer.[1] The KLS featured in the Scarfo case is different. Here, the FBI obtained authorization from the court to "deploy, maintain, utilize, and remove" the software, firmware, or hardware required to record the keystrokes to learn Scarfo's passphrase, on grounds that there was probable cause to believe that the encrypted file contained information relevant to their investigation of Scarfo.[2] They were authorized by court order to surreptitiously enter Scarfo's office, by breaking and entering if necessary, and to install their program without his knowledge. The order further authorized the government to break and enter as many times as needed during a 30-day period to maintain the software. Lastly, the court order allowed authorities to postpone notifying Scarfo of the order,

---

[1] *Carnivore: Will It Devour Your Privacy?* 2001 Duke L. & Tech. Rev. 0028 (2001), available at http://www.law.duke.edu/journals/dltr/articles/2001dltr0028.html. (last visited January 8, 2002).

[2] *Order Authorizing the Surreptitious Entry Into the Premises of Merchant Services of Essex County, Located at 149 Little Street, Belleville, New Jersey, For the Purpose of Conducting a*

because premature notification would "seriously compromise" the ongoing investigation.[3] After its installation, the KLS was in place for two months. The last thing it recorded was Scarfo's PGP passphrase.[4]

The Court's Review

New Jersey District Court Judge Politan referred to the case as presenting "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."[5] Politan added that "recent events" and national security concerns rendered the situation even more critical. One can only assume the "recent events" to which he refers to are the terrorist attacks of September 11.

The government investigation into Scarfo's activities became problematic when federal agents acting on search warrants and searched the offices of Scarfo and co-defendant Frank Paolercio. The agents seized several files from Scarfo's computer, but were prevented from accessing one of them due to Scarfo's use of an encryption program called PGP (i.e. "pretty good privacy"). Convinced that the file contained evidence of Scarfo's illegal activities, the FBI obtained an order from a magistrate judge to install its KLS on Scarfo's computer. A KLS operates by recording the keystrokes typed on a keyboard. The FBI was able to look at the KLS record obtained from Scarfo's computer and determine his PGP passphrase. Scarfo's passphrase happened to be the same as the Bureau of Prisons ID number assigned to his father, mob boss Nicodemo "Little Nicky" Scarfo, Sr.[6] The FBI used the passphrase to open the encrypted file, and subsequently indicted Scarfo using information they gained through their KLS search.[7]

Scarfo filed two motions: one motion for pretrial discovery seeking information about how the FBI's KLS system worked and another motion to suppress the evidence gleaned from the FBI's use of KLS. The motion to suppress the evidence rested on the grounds that it was a

---

Search For Evidence of Violations of Title 18, U.S.C. §§ 371, 892-894, 1955 and 1962, available at http://www2.epic.org/crypto/scarfo/order_6_99.pdf. (last visited January 8, 2002).

[3] *Id*.

[4] Rasch, Mark, *Break the Scarfo Silence*, available at http://www.businessweek.com/technology/content/sep2001/tc2001094_186.htm. (last visited January 8, 2002).

[5] *Id*. at 1.

[6] See Schwartz, John, *U.S. Refuses to Disclose PC Tracking*, available at http://www.nytimes.com/2001/08/25/technology/25CODE.html, (last visited January 8, 2002); Rasch, Mark, *Break the Scarfo Silence*, available at http://www.businessweek.com/technology/content/sep2001/tc2001094_186.htm. (last visited January 8, 2002).

general, not specific, search warrant in violation of the Fourth Amendment and that the KLS system was effectively an illegal wiretap.

Judge Politan expressed his concern that the FBI's system may run afoul of federal wiretapping statutes and ordered the government to file a brief explaining their KLS and its interaction with the functions of a computer. The government contended that disclosure of this information would raise severe national security concerns, and that the KLS system was classified and deserved protection under the Classified Information Procedures Act (CIPA).[8] The court then agreed to an *in camera, ex parte* hearing.

During this hearing, which was restricted to persons with top-secret and higher government clearances, government officials detailed the workings of the KLS system, including its operation in conjunction with a computer modem. Officials also presented their case that the revelation of the inner workings of the KLS in open court would present a threat to national security. Agreeing with the government as to the national security threat, Judge Politan issued a protective order in accordance with CIPA. The order sealed the records of the *in camera* review, and provided that the government would provide Scarfo with an unclassified summary of the workings of the KLS, so he could present a defense. The unclassified summary of KLS is in the form of an affidavit from Randall Murch, a Special Agent of the FBI working as Deputy Assistant Director of the FBI Laboratory Division's Investigative Technologies Branch.[9]

The Murch Affidavit

The Murch affidavit addresses the type of information recorded by the KLS. Murch said that the FBI was careful not to record or intercept electronic communications. "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."[10]

Murch provided some details as to how the FBI made sure it was not recording data sent through Scarfo's computer modem. He said that when each keystroke was made, the default setting of the KLS was *not* to record it, pending verification that each of the communication ports on Scarfo's computer was inactive, meaning that the computer modem was not in use and the

---

[7] *Id*.
[8] Classified Information Procedures Act, 18 U.S.C. App. III, § 1 (2001) .
[9] Affidavit of Randall S. Murch, available at http://www.epic.org/crypto/scarfo/murch_aff.pdf. (last visited January 8, 2002).
[10] *Id*. at 5.

computer was not transmitting any data.[11] Murch indicated that the FBI's use of the KLS in this manner was extremely cautious, pointing out that using the Microsoft Windows operating system, it is possible that a user may be working in one window online, for example, using a program like America Online, and simultaneously work in another window without electronic communication (for example, using a word processing document). Murch said that while it is entirely possible for this to happen, and for the user to be decrypting PGP files without communicating while the modem was activated. The FBI designed the KLS not to record any keystrokes that were typed while Scarfo's modem was operational. Eventually, the FBI learned that Scarfo's passphrase could not have been contained in an electronic communication anyway. Scarfo's configuration of his PGP program prevented his passphrase's transmission over a network. According to Murch, this 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."[12]

KLS's Potential for Over-inclusiveness

Despite the FBI's assurances that the KLS did not record communications, it still might be over-inclusive. The FBI, for all its good intentions, had no way of knowing whether Scarfo would use his computer keyboard to type his PGP passphrase or a letter to his attorney within the confidential and privileged attorney-client relationship. If use of the KLS becomes widespread, the FBI would potentially get a lot more information than authorized by their search warrants. The court addressed these concerns by likening the use of the KLS to the search of a file cabinet for a specific file. "…[I]t 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."[13] This argument is not compelling—the FBI did not determine whether each keystroke was an item to be seized, but rather seized them al and then determined whether they constituted the information sought.

What remains most disturbing about this case is that while the court knows the specifics of the KLS, Scarfo and the general public do not. The reasons for CIPA are not to be taken lightly, especially in light of our current environment, but it is possible that we are too quick to jump on the national security argument. We would do well to remain suspicious when the government keeps information from the public, asserting that it knows best. Logic dictates that

---

[11] *Id*. at 6-7.
[12] *Id*. at 8.
[13] Scarfo, 2001 WL 1650936, at *5 (*quoting United States v. Conley*, 4 F. 3d 1200, 1208 (3rd Cir. 1993)).

even in cases where the government is correct, the public will remain unsatisfied because the secrecy of the matter prevents an adequate explanation.

Even as he ruled on the pre-trial motions, Judge Politan was conscious of the tensions of the case:

> Modern-day criminals have also embraced technological advances and used them to further their felonious purposes. Each day, advanced computer technologies and the increased accessibility to the internet means criminal behavior is becoming more sophisticated and complex…as a result of this surge in so-called 'cyber-crime,' law enforcement's ability to vigorously pursue such rogues cannot be hindered where all Constitutional limitations are scrupulously observed.[14]

Yet what he said a few sentences before is perhaps even more compelling. "We must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology."[15]

Ever vigilant, indeed. Since there can be no interlocutory appeal of this decision, we all eagerly await the trial, and what is sure to be a subsequent appeal to the Third Circuit.

By: Angela Murphy

---

[14] Scarfo, *supra note 13*, at *10.
[15] *Id*.