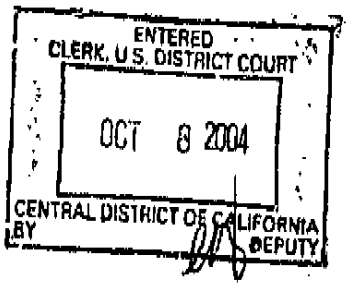

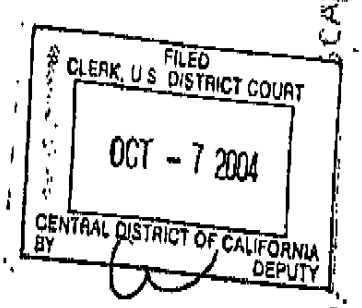

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. LARRY LEE ROPP, Defendant.	**Case No. CR 04-300-GAF** **ORDER RE: MOTION TO DISMISS**

I.

INTRODUCTION

In the present case, a federal grand jury indicted defendant Ropp for allegedly attempting to intercept electronic communications in violation of 18 U.S.C. § 2511(1)(a) by installing a device, called a KeyKatcher, on the desktop computer of Karen Beck at the Orange County offices of Bristol West Insurance Group/Coast Nation Insurance Company. For purposes of this motion, the parties agree that Ropp placed the KeyKatcher on the cable that connects Ms. Beck's keyboard to her computer's central processing unit (CPU). As Ms. Beck composed e-mails and other messages by depressing

keys on the keyboard (an act known to some of us as "typing"), the KeyKatcher recorded and stored the electronic impulses traveling down the cable between her keyboard and the computer to which it was attached. The KeyKatcher, in this way, "eavesdrops" on the person typing messages into the computer.

After the KeyKatcher has performed its "eavesdropping function," anyone who obtains possession of the device can recover, from its memory, the stored impulses and convert them to text. The KeyKatcher therefore enables a person who has possession of the device to determine what messages have been typed on the keyboard.

Defendant now moves to dismiss the indictment on the ground that, even assuming that the factual allegations of the indictment are true, the conduct alleged does not constitute an "interception" of "electronic communications" within the meaning of Section 2511, and therefore does not constitute a crime within the meaning of the statute. Although the Court disagrees with the thrust of Defendant's argument – that no communication was "intercepted" – the Court concludes that the motion should be **GRANTED** because the transmission of keystrokes from a keyboard to a computer's processing unit is not the transmission of an electronic signal by a system that affects interstate commerce, and therefore does not constitute an "electronic communication" within the meaning of the statute.

II.

FORMULATING THE ISSUE

Defendant contends that, given the definition of the key terms of Section 2511, the KeyKatcher does not "intercept" "electronic communications" within the meaning of the statute. See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003); United States v. Smith, 155 F.3d 1051 (9th Cir. 1998). According to defendant, the KeyKatcher intercepts electronic signals created by a computer keyboard as word

processing documents, e-mails and other communications are being prepared, but before they are transmitted. Defendant argues that the e-mails, and other communications that were later sent (and not intercepted) are "electronic communications" under the act, but that the prosecution cannot base its case on the interception of the key strokes that created them. According to Defendant, this is because the interception must be contemporaneous with the communication and must involve transmissions that affect interstate or foreign commerce. See, e.g., Smith, 155 F.3d, at 1057; Konop, 302 F.3d at 878.

The Government opposes the motion contending that Defendant has misinterpreted the Wiretap Act. The Government argues that the electronic signals from the keyboard to the computer were "electronic communications" within the meaning of the Act because the KeyKatcher "literally stripp[ed] communication off a wire as the communication was being transmitted from one point to another." (Opp'n, at 2.) The Government contends that the acquisition of the communication did not occur prior to, but during the transmission of these electronic signals and that, therefore, the alleged "contemporaneity" requirement has been met.

The Court concludes that neither party has squarely focused on the real issue in this case. The Defendant contends that no interception occurred and therefore gives insufficient attention to the meaning of "electronic communication." The Government is quite willing to accept defendant's relative disinterest in discussing "electronic communication," in all likelihood because the ease with which the "no interception" argument can be overcome. In that regard, no one disputes, for purposes of this motion, that the KeyKatcher was installed on Ms. Beck's computer. Likewise, no one disputes that the KeyKatcher intercepted the wire transmission of electronic signals as they passed from Ms. Beck's keyboard into her computer. Further, the Government does not, in its opposition, contend that the e-mails or other

communications were themselves intercepted. In short, the record establishes beyond argument that the KeyKatcher intercepted electronic signals.

But that conclusion is not the end of the argument, but merely the end of its beginning and brings the Court to the heart of the matter – whether or not the intercepted signals constitute "electronic communications" within the meaning of the Act. As discussed below, this question is more complex than it might seem at first because the term is bound up with the jurisdictional element of the statute and requires that the transmission be made by a system that affects interstate commerce. The Court must therefore consider whether internal computer transmissions can be viewed as transmissions by a system that affects interstate commerce to determine whether they constitute "electronic communications" under the Wiretap Act.

III.

DISCUSSION

A. RULE 12

Although Defendant does not identify the authority for the present motion, it appears that the motion is made under Rule 12(b), FED. R. CRIM. P. which authorizes the Court to resolve "any defense, objection, or request which is capable of determination with the trial of the general issue . . . ." The rule apparently permits a defendant to move to quash an indictment for failure to state an offense. Ex Parte Parks, 93 U.S. 18, 20 (1876). Thus, if no statute makes the alleged offense a crime, a defendant may challenge that defect under Rule 12. See Id.

In this case, the Indictment, on its face, is not susceptible to such a challenge. However, the parties have agreed on certain facts that have been developed in discovery to permit the Court to consider this motion without waiting until the conclusion of the Government's case-in-chief. The Court will proceed to consider the motion on the basis of the uncontested facts.

B. THE STATUTORY LANGUAGE

In cases of statutory construction the Court begins with the text of the statute. Hughes Aircraft Co. v. Jacobson, 525 U.S. 432, 438 (1999). The Court attempts to determine the meaning of words and phrases from the context in which they are used. United States v. Councilman, 373 F.3d 197, 200 (1st Cir. 2004). Nevertheless, statutory interpretation has its limits. As the court in Councilman stated in addressing the statute in dispute in this case:

> The Wiretap Act's purpose was, and continues to be, to protect the privacy of communications. We believe that the language of the statute makes clear that Congress meant to give lesser protection to electronic communications than wire and oral communications. Moreover, at this juncture, much of the protection may have been eviscerated by the realities of modern technology. We observe, as most courts have, that the language may be out of step with the technological realities of computer crimes. However, it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly.

373 F.3d at 203-04.

With these principles in mind, the Court turns to the language of the statute.

Section 2511 provides in pertinent part:

> 1) Except as otherwise specifically provided in this chapter any person who--
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> . . . .
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 USC § 2511(1)(a)(2004).

Section 2510 contains several definitions that bear on the Court's analysis:

> As used in this chapter--

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

. . . .

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include–

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510 (2004).

The definition of "electronic communication" was added in 1986 when Congress passed the Electronic Communication Privacy Act (ECPA). Pub. L. No. 99-508, Title I, §§ 101-02, 100 Stat. 1849053 (1986). As Defendant correctly notes, Congress intended, as one of the purposes of the ECPA, to extend to "electronic communications" many of the protections afforded "wire communications" under the original Wiretap Act. The statute clearly distinguishes between the two types of communications and establishes that the two types of communication are mutually exclusive. 18 U.S.C. § 2510(12)(A). Motivated by significant changes in communications technology, the principal objective of the statute was to place electronic communications on

the same footing as wire communications. Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995) ("By these 1986 amendments, authority to intercept electronic communications became subject to the same requirements as those applicable to the interception of oral and wire communications.")

However, stating the objective of the ECPA provides little help in answering the question now before the court. Likewise, as discussed below, the case law offers little guidance in these circumstances. The Court will therefore seek to clearly state the facts of the violation alleged in the pending indictment, and glean what guidance it can from the case law in the area.

B. ANALYSIS

1. The Government's Position Re: "Electronic Communications"

Since the parties agree that electronic signals were transmitted from Ms. Beck's keyboard, and since the record establishes that, between the keyboard and the destination of the signals, an interception occurred, the Court must determine whether the signals that were intercepted were "electronic communications" within the meaning of the statute. That determination turns on whether the signals were transmitted "by a system . . . that affects interstate or foreign commerce."

The Government takes a broad view of this language, and contends that, based on its proffer, the Court must deny the motion. The Government proffers that Ms. Beck arrives at work each day, turns on her computer, and "logs on" to a network that connects her to a server that, in turn, is connected to other servers that are a part of the company's nationwide computer network. The Government acknowledges that, before any e-mail message or other communication is sent through the network, the message must be composed on Ms. Beck's local computer and then transmitted, upon Ms. Beck's command, through the network. Thus, according to the Government's proffer, when Ms. Beck enters data through her keyboard, she is communicating with

her own computer, not with the server or any other computer in the company's network.

In the Government's view, no significance should be given to the fact that the transmission is internal to Ms. Beck's computer. Rather, the Government contends that Ms. Beck's transmission of signals to her computer was transmitted by a system that affects interstate or foreign commerce because she was "logged on" to the network. Nothing more need be shown, according to the Government, because the phrase "electronic communication" does not require the interception of signals transmitted *in* interstate or foreign commerce.[1] For that reason, the Government takes the position that any signal transmitted from a keyboard to a computer with an internet connection constitutes an "electronic communication" within the meaning of the statute, whether or not the internet connection was activated at the time of the transmission, because the system by virtue of that connection "affects interstate or foreign commerce."[2]

---

[1]The Government also contends that, to the extent that the definition requires a transfer of signals that "affect commerce," the communications in this case fit the definition because the communications that were captured consisted of e-mails and communications to the company's database. (Opp'n., at 4 n. 4.) The argument suffers from a critical flaw – the communications in question involved the preparation of e-mails and other communications, but were not themselves e-mails or any other communication at the time of interception. At the time of interception, they no more affected interstate commerce than a letter, placed in a stamped envelope, that has not yet been mailed. Cf. United States v. Robinson, 545 F.2d 301, 304 (2d Cir. 1976) (theft of mail conviction reversed where no evidence presented that items actually placed in the mail). Indeed, this aspect of the Government's argument plays directly into the Defendant's "no interception" argument. Clearly, the e-mail and database communications were not "intercepted" by the KeyKatcher because they had not yet been sent.

[2]The Government asserted this position at the hearing on the motion. The Government's view is that the only internal computer communications that do not constitute "electronic communications" are those made on computers that are not connected either to the internet or some other network of computers. The connection to the internet or the network, not the transmission over the network, is the critical fact in the Government's view.

The court in Scarfo concluded, without expressly addressing the language under discussion in this case, that the Act would apply only to those signals transferred through the modem and over a telephone or cable and, therefore, the interceptions should not be suppressed. Id. at 582.

Though the reasoning of Scarfo is flawed in some respects, its discussion of facts that are analogous to those presented in this case provides some support for the proposition that the transmission of signals within a computer do not constitute "electronic communications" within the Act.

3. United States v. Councilman

At the hearing, defense counsel argued that United States v. Councilman, 373 F.3d 197 (1st Cir. 2004) considered and rejected the Court's tentative views on the meaning of "electronic communications." Councilman, however, addresses the acquisition of stored electronic data, though in a context that provides some additional insight into the issue now before the Court.

In Councilman, the Government obtained an indictment against employees of an e-mail service provider for acquiring all incoming e-mails directed to Amazon.com in violation of the Wiretap Act. The parties agreed to the following facts regarding the transmission of e-mails:

> An e-mail message, which is composed using an e-mail program, is transferred from one computer to another on its way to its final destination, the addressee. Building on the principle of store and forward, the message is handed to a Message Transfer Agent ("MTA") which stores the message locally. The message is routed through the network from one MTA to another until it reaches the recipient's mail server, which accepts it and stores it in a location accessible to the recipient. Once the e-mail is accessible to the recipient, final delivery has been completed. The final delivery process places the message into storage in a message store area. Often, a separate Mail Delivery Agent ("MDA") will be required to retrieve the e-mail from the MTA in order to make final delivery.

---

[3](...continued)
computer system.

The Court has identified two cases, among the many that have interpreted the Wiretap Act, that provide some guidance, although for reasons that are apparent from the discussion of those cases, are not controlling.

2. *United States v. Scarfo*

The only case to analyze a keystroke capturing device implicitly rejected the government's argument. United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001). In Scarfo, the court addressed a motion to suppress evidence of signals intercepted by the FBI through a keystroke capturing device, called a KLS, which was placed on the defendant's computer. Id. At 574. Because the computer was connected to the internet through a modem, the District Court expressed concern over whether the device intercepted keystrokes transmitted through a modem and over a telephone or cable line. Id. at 581-82. Accordingly, the court conducted an inquiry into the operation of the KLS to determine whether or not it captured such transmissions. Describing the conduct of the FBI, the court wrote:

> 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 transmitted in real time via the communication ports. See Murch Aff., ¶ 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 that the modem was not using any port at that time, then the keystroke in question would be recorded.

Id. (Emphasis added).[3]

---

[3]It appears that the District Court inadvertently interchanged the terms "electronic communications" and "wire communications" in its discussion of the interception issue. However, the discussion in the quoted passage regarding the operation of the KLS device suggests that the Court understood that it was dealing not with "wire communications" as defined in the act but rather "electronic communications," that is, the transmission of electronic signals through the

(continued...)

The court in Scarfo concluded, without expressly addressing the language under discussion in this case, that the Act would apply only to those signals transferred through the modem and over a telephone or cable and, therefore, the interceptions should not be suppressed. Id. at 582.

Though the reasoning of Scarfo is flawed in some respects, its discussion of facts that are analogous to those presented in this case provides some support for the proposition that the transmission of signals within a computer do not constitute "electronic communications" within the Act.

3. United States v. Councilman

At the hearing, defense counsel argued that United States v. Councilman, 373 F.3d 197 (1st Cir. 2004) considered and rejected the Court's tentative views on the meaning of "electronic communications." Councilman, however, addresses the acquisition of stored electronic data, though in a context that provides some additional insight into the issue now before the Court.

In Councilman, the Government obtained an indictment against employees of an e-mail service provider for acquiring all incoming e-mails directed to Amazon.com in violation of the Wiretap Act. The parties agreed to the following facts regarding the transmission of e-mails:

> An e-mail message, which is composed using an e-mail program, is transferred from one computer to another on its way to its final destination, the addressee. Building on the principle of store and forward, the message is handed to a Message Transfer Agent ("MTA") which stores the message locally. The message is routed through the network from one MTA to another until it reaches the recipient's mail server, which accepts it and stores it in a location accessible to the recipient. Once the e-mail is accessible to the recipient, final delivery has been completed. The final delivery process places the message into storage in a message store area. Often, a separate Mail Delivery Agent ("MDA") will be required to retrieve the e-mail from the MTA in order to make final delivery.

---

[3](...continued)
computer system.

Id. at 199.

The facts before the Court established that the defendants wrote a program that allowed them to acquire the targeted e-mails from their MDA before the messages were read by the intended recipient. Id. However, the program operated only within the confines of the provider's computer. Id. When the relevant programs performed operations affecting the e-mail system, the messages existed in the random access memory (RAM) or in hard disks, or both, within the provider's computer systems. Id.

At the trial court level:

> Defendant moved to dismiss the Indictment for failure to state an offense under the Wiretap Act, as the e-mail interceptions at issue were in "electronic storage," as defined in 18 U.S.C. § 2510(17), and could not be intercepted as a matter of law. The district court did not initially grant the motion to dismiss but, upon further briefing by the parties, granted the motion and dismissed Count One. The district court found that the e-mails were in electronic storage and that, therefore, the Wiretap Act could not be violated because the requisite "interception" was lacking.

Id. At 200. (Citing United States v. Councilman, 245 F. Supp.2d 319 (D. Mass. 2003). The trial court granted the motion and the circuit court affirmed. Id. at 204. The reviewing court held that, even though the e-mails were in the process of being transmitted from sender to the addressee, they were, at the moment when they were acquired by the defendants, in storage. Id. at 203. Therefore, the use of a program within the defendant's own computer to obtain data temporarily resident at that location was held not to violate the Wiretap Act.

4. The Limits and Import of the Decisions

Neither Scarfo nor Councilman, nor any other case cited by either party, squarely addresses the question presented in the present motion. Nevertheless, while Scarfo did not focus on the meaning of, and potential limitations inherent in, the definition of "electronic communication," it indicates

the importance the trial court placed on determining whether the intercepted keystrokes were transmitted within, or beyond, the defendant's computer. Because the intercepted keystrokes were not transmitting beyond the computer, the trial court held that the provisions of the Wiretap Act did not apply. Councilman, on the other hand, looked past the fact that the communications in issue were in route, over a system that affects interstate or foreign commerce, and focused on the fact that the communications were temporarily stored and therefore were not "intercepted" within the meaning of the Wiretap Act. But if an electronic communication which is in the process of transit, even if momentarily "parked" in an electronic lot, can be acquired without violating the Act, this Court finds it difficult to conclude that the acquisition of internal computer signals that constitute part of the process of ***preparing*** a message for transmission would violate the Act. Indeed, these internal computer signals can only be encompassed by the Act if the "system" of transmission affects interstate commerce.

Informed by the decisions discussed in this memorandum, and the many cases cited in the papers submitted by the parties, the Court concludes that the communication in question is not an "electronic communication" within the meaning of the statute because it is not transmitted by a system that affects interstate or foreign commerce. The "system" involved consists of the local computer's hardware – the Central Processing Unit, hard drive and peripherals (including the keyboard) – and one or more software programs including the computer's operating system (most likely some version of Microsoft Windows although other possibilities exist), and either an e-mail or other communications program being used to compose messages. Although this system is connected to a larger system – the network – which affects interstate or foreign commerce, the transmission in issue did not involve that system. The network connection is irrelevant to the transmissions, which could have

been made on a stand-alone computer that had no link at all to the internet or any other external network. Thus, although defendant engaged in a gross invasion of privacy by his installation of the KeyKatcher on Ms. Beck's computer, his conduct did not violate the Wiretap Act. While this may be unfortunate, only Congress can cover bases untouched. Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 114 (3rd Cir. 2004); see also United States v. Stelger, 318 F.3d 1039, 1049 (11th Cir.), cert. denied, 538 U.S. 1051 (2003) (courts cannot create remedy where Congress had established none).

For these reasons, the conduct described in the indictment fails to state the elements of a crime under the Wiretap Act. The indictment and the charges set forth against the defendant therein, are therefore **DISMISSED.**

IV.

CONCLUSION

For the reasons set forth above, the indictment is **DISMISSED.**

IT IS SO ORDERED.

DATED: October 6, 2004

Judge Gary Allen Feess
United States District Court