IN THE UNITED STATES COURT FOR THE DISTRICT OF UTAH
CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. BRYAN VANCE JONES, Defendant.	MEMORANDUM DECISION DENYING MOTION TO COMPEL UNDER WIRETAP ACT Case No. 2:04-CR-00510 PGC

On January 11, 2005, this court held a hearing to consider defendant Bryan Jones' motion to suppress evidence in connection with an authorized search warrant. This court denied Mr. Jones' motion on Fourth Amendment grounds, but left open the possibility that the evidence might be suppressed under the Federal Wiretap Act.[1] On consideration, this court decides that Mr. Jones' email communications cannot be suppressed because the Act does not provide for suppression of electronic communications.

BACKGROUND

On June 15, 2004, agents of the Federal Bureau of Investigations met with a confidential informant who gave them an envelope containing copies of printed email messages from Jones'

[1] 18 U.S.C. §§ 2510-22.

email accounts. Based on that information, the agents obtained a warrant to search Mr. Jones' email accounts and computer.

Before the court now is Mr. Jones' claim that the confidential witness may have violated the Federal Wiretap Act by accessing Mr. Jones' personal email accounts. Mr. Jones urges this court to suppress any evidence obtained in violation of the Act (such as the email messages originally provided to the FBI agents), as well as any other derivative evidence (such as the email communications obtained pursuant to the search warrant).

To support his motion to suppress, Mr. Jones moved to compel discovery of the identity of the informant witness and the means by which the informant accessed Mr. Jones' private email communications. To protect the safety of that informant, this court refused to order disclosure of the information for reasons stated at greater length in the sealed transcript. Nonetheless, this court articulated a "hypothetical" containing the relevant facts to provide Mr. Jones sufficient basis for presenting his claim about the Wiretap Act. According to the hypothetical, Mr. Jones used a computer at a local public library in order to access his email account. After leaving the library computer station, Mr. Jones' email account remained accessible, and a librarian discovered the email messages in Mr. Jones' account. Mr. Jones argues that these facts constitute a violation of the Wiretap Act that should lead to the suppression of evidence. The court disagrees.

DISCUSSION

Title III of the Omnibus Crime and Control and Safe Street Act of 1968 (the "Wiretap Act" or the "Act"),[2] as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"),[3] prohibits the intentional interception and disclosure of any wire, oral, or electronic communications.[4] Unlike the Fourth Amendment,[5] the Act applies to not only government agents but also to private individuals.[6] Here, whether the confidential informant unlawfully intercepted Mr. Jones' private email correspondence is a complicated factual inquiry that is ultimately irrelevant to this motion. In order to prove a violation of the Wiretap Act, Mr. Jones would have to prove that the informant acted *intentionally*[7] and that his email messages were *intercepted*[8] contemporaneous to their transmission.[9] This court's order preserving the informant's

---

[2] 18 U.S.C. §§ 2510–22.

[3] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[4] *See* 18 U.S.C. § 2511(1).

[5] *See generally* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich.L.Rev. 801 (2004).

[6] *See* 18 U.S.C. § 2511(1) (prohibiting "any person").

[7] *See* 18 U.S.C. § 2511(1)(a).

[8] *See* 18 U.S.C. § 2511(1).

[9] *See, e.g.*, *United States v. Councilman*, 373 F.3d 197, 201-03 (1st Cir. 2004), *reh'g granted*, 385 F.3d 793 (holding that copying emails at the server level was not an interception and citing with approval circuit court decisions requiring interception to be contemporaneous with transmission); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003), *cert. denied*, 538 U.S. 1051 (2003) ("[W]e hold that a contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications."); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003)("We therefore hold that for a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."); *Steve Jackson Games Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994) (holding that seizure of stored but unread email messages was not an interception and citing with approval the lower court's requiring interception to be contemporaneous with transmission). *But see Konop v. Hawaiian Airlines, Inc.*, 302 F.3d

confidentiality necessarily complicates investigating the facts surrounding these elements. It is, however, unnecessary to investigate those facts because the Wiretap Act's suppression remedy would be unavailable to Mr. Jones even if the informant unlawfully intercepted his messages. The Wiretap Act's suppression remedy is not coextensive with its general prohibitions of conduct. Although unauthorized interception of electronic communications is unlawful under § 2511, there is no provision for the suppression of intercepted electronic communications under the Act.

Whether the Wiretap Act's suppression remedy, § 2515, extends to electronic communications is a question of first impression in the Tenth Circuit. The Act's plain text, however, is unambiguous, leaving little room for argument. In 1986, Title I of the ECPA amended the federal Wiretap Act to include electronic communications.[10] Previously, the Act had only applied to the interception of wire and oral communications. However, as the Eleventh Circuit has noted,[11] "[d]espite the fact that the ECPA amended numerous sections of the Wiretap Act to include 'electronic communications,' the ECPA did not amend § 2515."[12]

Section 2515 provides the sole suppression remedy for unlawfully intercepted communications.

868, 886 (9th Cir. 2002) (Reinhardt, J., concurring in part, dissenting in part) ("I dissent, however, from Part B of Section I, which holds that the term 'intercept' in the Wiretap Act, as applied to electronic communications, refers solely to contemporaneous acquisition.").

[10] *See* Pub. L. No. 99-508, 100 Stat. 1848; S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[11] *Steiger*, 318 F.3d at 1039.

[12] *Id.* at 1050.

> Whenever *any wire or oral communication* has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.[13]

Moreover, the Eleventh Circuit has also noted that "although . . . Congress considered amending § 2515 in the USA Patriot Act to 'extend[] the statutory exclusion rule in 18 U.S.C. § 2515 to electronic communications,' the Act was passed without such an amendment."[14] Thus, even though § 2511 prohibits the interception and disclosure of "any wire, oral, or *electronic* communication,"[15] the suppression remedy in § 2515 applies only to intercepted wire and oral communications. Mr. Jones does not contest that email correspondence is properly classified as electronic communications. Therefore, the Wiretap Act affords Mr. Jones no basis for suppressing either his personal email correspondence or any corresponding derivative evidence, as both the Eleventh and Sixth Circuits have held.[16]

---

[13] 18 U.S.C. § 2515 (emphasis added).

[14] *Steiger*, 318 F.3d at 1050 (comparing H.R. Rep. No. 236(I), at 8 (2001), with USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)).

[15] 18 U.S.C. § 2511(1) (emphasis added).

[16] *Steiger*, 318 F.3d at 1050–51 (declining to suppress electronic communications obtained by unauthorized hacking because "[s]uppression is not a remedy under the Wiretap Act with respect to unlawfully seized electronic communications"); *United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990) (declining to suppress evidence obtained from an allegedly intercepted telephone number from a pager because the Wiretap Act "does not provide an independent statutory remedy of suppression for interceptions of electronic communications").

Notwithstanding Mr. Jones' concession that the language of § 2515 is "unambiguous,"[17] he argues nonetheless that § 2517(3), by negative implication, provides for the suppression of electronic communications.[18] Section 2517(3) reads:

> Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

Mr. Jones asserts that this provision "suggests that any wire, oral, or electronic communication that was illegally intercepted cannot be used in a court proceeding."[19] In essence, Mr. Jones argues that, because § 2517(3) permits disclosure at a judicial proceeding of the contents of intercepted electronic communications when the contents were received by authorized means, the converse is also true–that is, that electronic communications not intercepted by authorized means are necessarily excluded from testimony at a judicial proceeding.

Mr. Jones' interpretation of the import of § 2517(3) is flawed for several reasons. To begin, Rule 402 of the Federal Rules of Evidence require that "[a]ll relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority."[20] Mr. Jones does not point to an "Act of Congress" that would authorize repeal of the Rule's express mandate to admit all relevant evidence; rather, he asks this court to find that §

---

[17] *See* Defendant's Memorandum Regarding Application of Wiretap Act at 4.
[18] *See id.* at 5–6.
[19] *Id.* at 5.
[20] FED. R. EVID. 402.

2517(3) repeals Rule 402 by negative implication. In its most recent discussion of repeal by implication, the Tenth Circuit noted:

> The Supreme Court has 'repeatedly stated . . . that absent a clearly expressed congressional intention, repeals by implication are not favored. An implied repeal will only be found where provisions in two statutes are in irreconcilable conflict, or where the latter act covers the whole subject matter of the earlier one and is clearly intended as a substitute.'[21]

Because § 2517(3) is neither in irreconcilable conflict with or a substitute for Rule 402, this court will not read more into § 2517(3) than the import of the plain text.

Moreover, it is clear from the general context of § 2517(3) that it does not create by implication a suppression remedy for electronic communications. Read in context, § 2517 describes the limited purposes for which communications received by authorized means may be used or disclosed; its effect has no implication for communications received by unauthorized means. Without § 2517, the wiretaps authorized by § 2516 would be of little use. Thus, § 2517 puts § 2516 into effect, by granting permission for the disclosure of otherwise privileged communications that were acquired by means of an authorized wiretap. Under § 2517, investigative and law enforcement officers may disclose the content of lawfully intercepted communications to other officers[22] and may otherwise use such content to perform official duties;[23] similarly, any person who has received lawfully intercepted communications may disclose the content of those communications while giving testimony.[24] Thus, without § 2517,

---

[21] *United States v. Hahn*, 359 F.3d 1315, 1321(10th Cir. 2004) (citing *Branch v. Smith*, 538 U.S. 254, 273 (2003) (omission in original)).

[22] *See* 18 U.S.C. § 2517(1).

[23] *See* 18 U.S.C. § 2517(2).

[24] *See* 18 U.S.C. § 2517(3).

the privileged nature of information obtained by means of a lawful wiretap would frustrate the purposes of obtaining the authorized wiretap in the first place; thus, section 2517 abrogates the privilege attached to the intercepted information. If there is any negative implication of § 2517(3) with regards to electronic communications, it is only that electronic communications received by means of an authorized wiretap are nonetheless privileged and may not be disclosed (without an express grant of statutory authority). Section 2517 does not, however, suggest by negative implication that electronic communications unlawfully intercepted should be suppressed.

The plain language of § 2518(10)(c) and its surrounding legislative history remove any doubt regarding the alleged negative implication of § 2517(3) or any other suggestion that electronic communications may be suppressed. Section 2518(10)(c) states unequivocally, "The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the *only* judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications."[25] The Senate Report accompanying the ECPA makes clear the limited reach of the exclusionary rule, "The purpose of [§ 2518(10)(c)] is to underscore that, as a result of discussions with the Justice Department, the Electronic Communications Privacy Act does not apply the statutory exclusionary rule contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the interception of electronic communications."[26] After reviewing this legislative history, the Eleventh Circuit was satisfied that no implied suppression remedy existed: "[t]he omission of 'electronic communications'

---

[25] 18 U.S.C. § 2518(10)(c) (emphasis added).

[26] S. Rep. No. 99-541, at 23, 1986 U.S.C.C.A.N. at 3577, *quoted in United States v. Steiger*, 318 F.3d 1039, 1051–52 (11th Cir. 2003).

from section 2515 is dispositive. The Wiretap Act does not provide a suppression remedy for electronic communications unlawfully acquired under the Act."[27] In sum, Mr. Jones may not suppress evidence obtained from the interception of his personal email account because the Wiretap Act's suppression remedy, § 2515, does not apply to the interception of electronic communications.

Finally, Mr. Jones raises the possibility that the confidential informant accessed Mr. Jones' email accounts after intercepting his password by means of an unlawful *wire or oral interception*.[28] Mr. Jones hypothesizes that "suppression would be available pursuant to 18 U.S.C. § 2515 . . . if the informant eavesdropped or listened in on one of Mr. Jones' phone conversations or placed herself in a position where she intercepted oral communications."[29] Thus, Mr. Jones argues that, if the informant indeed intercepted Mr. Jones' email password in such manner, then Mr. Jones' email communications "derived therefrom" may be properly suppressed under § 2515.[30] Mr. Jones' argument is at least plausible. If the informant intercepted a wire or oral communication, which revealed Mr. Jones' email password, then Mr. Jones' email communications, which were obtained by means of the password, are likely subject to suppression.

---

[27] *Steiger*, 318 F.3d at 1052; *see also*, WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, CRIMINAL PROCEDURE, § 4.6 at 291 (4th ed. 2000) (exlusionary provisions limited only to violations having to do with wire or oral communications).

[28] Defendant's Memorandum Regarding Application of Wiretap Act at 7.

[29] *Id.*

[30] 18 U.S.C. § 2515 ("Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and *no evidence derived therefrom* may be received in evidence . . . ." (emphasis added)).

Several factors suggest, however, the unlikelihood of Mr. Jones' hypothesized scenario. To begin, the informant may have discovered Mr. Jones' password in numerous ways that do not implicate the Wiretap Act. Mr. Jones may have left his password written on a note or visible on a computer screen. Alternatively, the informant may not have needed Mr. Jones' password because the email program had been left open or the password had appeared automatically from computer memory (many current programs prompt users to allow the host computer to remember the password upon startup in order relieve the user from entering the password every time the programs is accessed). Finally, an unlawful interception requires the "use of [an] electronic, mechanical, or other device."[31] Thus, if the informant merely "eavesdropped" behind a closed door, as Mr. Jones seems to suggest, then the password was not intercepted; the informant must have used some form of device in order to have intercepted the password.

In any case, the government has now filed a pleading under seal which proves that the informant did not obtain information to access Mr. Jones' email account by intercepting any wire or oral communications through the use of a mechanical, or other device.

[31] 18 U.S.C. § 2510(4) (defining intercept as "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").

CONCLUSION

Mr. Jones' email communications (both those originally obtained by the informant and those derivative communications subsequently obtained pursuant to the search warrant) may not be suppressed because § 2515 does not apply to electronic communications, and there is no other applicable suppression remedy under the Wiretap Act. Additionally, because the informant in this case did not intercept any wire or oral communication of Mr. Jones' password (or other information used to access his email account) by means of some device, Mr. Jones' motion to suppress evidence pursuant to the Wiretap Act [30-1] IS HEREBY DENIED.

DATED this 12th day of April, 2005.

BY THE COURT:

/S/
Paul G. Cassell
United States District Judge

asp

United States District Court
for the
District of Utah
April 12, 2005

* * CERTIFICATE OF SERVICE OF CLERK * *

Re: 2:04-cr-00510

True and correct copies of the attached were either mailed, faxed or e-mailed by the clerk to the following:

Michele M. Christiansen, Esq.
US ATTORNEY'S OFFICE
,
EMAIL

Paul G. Amann, Esq.
UTAH ATTORNEY GENERAL'S OFFICE
CHILDREN'S JUSTICE DIVISION
5272 COLLEGE DR STE 200
SALT LAKE CITY, UT 84123
EMAIL

Mr Richard P Mauro, Esq.
43 E 400 S
SALT LAKE CITY, UT 84111
EMAIL

United States Marshal Service
DISTRICT OF UTAH
,
EMAIL

US Probation
DISTRICT OF UTAH
,
EMAIL