United States v. Bryan Vance Jones: CONSTITUTIONAL DEFECTS IN STATUTORY SUPPRESSION REMEDY IN THE CONTEXT OF PRIVACY

I. Introduction

In United States v. Jones,[1] the District Court held that the defendant could not suppress the e-mail messages obtained by informant in violation of the Title III of the Omnibus Crime and Control and Safe Street Act of 1968 ("Wiretap Act")[2] as amended by the Electronic Communications Privacy Act of 1986 ("ECPA").[3] The ECPA amended the Wiretap Act to include not only the prohibition of the intentional interception and disclosure of oral and wire communications but also electronic communications.

This comment explores the Wiretap Act's constitutionality or legitimacy in light of the Fourth Amendment protections. More specifically, the comment focuses on the injustice created by a statute that punishes the violator but does not remedy the harm suffered by the victim. Further, this comment will address the suppression remedy's failure to keep with the times by excluding electronic communications such as unlawfully obtained e-mail messages.

While keeping in mind the courts interests in refraining to act as a super-legislature, this comment will set out reasons why the court should have looked beyond the plain language of

[1] 364 F.Supp.2d 1303 (D.Utah 2005).

[2] 18 **U.S.C.** §§ 2510-22(2006).

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

the statute and afforded a Constitutional remedy for the defendant.

The court circumvents the issue of addressing the violation of the Wiretap Act – "whether the confidential informant unlawfully intercepted Mr. Jones' private email correspondence is a complicated factual inquiry that is ultimately irrelevant to this motion."[4] Instead, the court assumed that the e-mail correspondence was unlawfully intercepted and focuses on whether the Wiretap Act provides a suppression remedy.

Although the Wiretap Act prevents interception of illegally intercepted electronic communication, the court said once the e-mail is intercepted, the defendant must use a suppression remedy to prevent the e-mail from being allowed in as evidence.[5] Consequently, the unlawfully intercepted e-mail messages were admitted because the statute's literal language does not cover the suppression of electronic communications.

The court's focus on the conclusion that "the Wiretap Act's suppression remedy would be unavailable to Mr. Jones even if the informant unlawfully intercepted his messages"[6] reveals the court's failure to look beyond the plain language of the statute and to the U.S. Constitution. In Griswold v. Connecticut, "the

[4] United States v. Jones, 364 F.Supp.2d at 1305 (D. Utah 2005).

[5] Id.

[6] Id. at 1306.

Supreme Court has interpreted the U.S. Constitution as providing a fundamental 'right to privacy', located within the undefined 'penumbras' of the Bill of Rights."[7] While the U.S. Constitution does not explicitly mention privacy, the protection of privacy exists as evidenced by the combination of the different protections afforded by First, Third, Fourth, and Fifth Amendments.[8] As a result, the notion of "personal liberty contained in the Bill of Rights guarantees a 'right to privacy'

---

[7] Katherine A. Oyama, **E-Mail Privacy After United States v.Councilman: Legislative Options For Amending ECPA**, 1 Berkeley Tech L.J. 499 (2006), (citing Griswold v. Connecticut, 381 U.S. 479, 483-85 (1965) (stating that the U.S. Constitution protects the right to privacy although its text does not explicitly reference the term "privacy"). For example, privacy is protected by the First Amendment's freedom of association clause and guarantee of the right to speak anonymously, the Third Amendment's protection for privacy of the home, the Fourth Amendment's guarantee that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures ..." and the Fifth Amendment's right against self-incrimination. Daniel J. Solove & Marc Rotenberg, Information Privacy Law 20-21 (2003) (citing U.S. Const. amends. I, III-V).

[8] Id.

encompassing both 'explicit protection against government intrusion into the home and personal effects.'"[9]

With these weighty constitutional protections in the background, rather than focus on the aspect of privacy granted to the citizen, the court overlooks the constitutional protections and centers around the absence of an applicable suppression remedy in the plain language of the Wiretap Act.[10] Regardless of whether the electronic communication had been illegally intercepted, the court denies the defendant a remedy for violation of his right to privacy. In its literal reading, the suppression remedy within the Wiretap Act does not give an equal remedy to electronic communications as it does to oral or wire communications.[11] As a result, defendant's motion to suppress was denied on Fourth Amendment grounds.[12]

II. Background

The defendant, Mr. Jones, sought to suppress evidence turned over to the FBI by an informant.[13] The evidence that the

---

[9] See id., (citing Will Thomas DeVries, Note, Protecting Privacy in the Digital Age, 18 Berkeley Tech. L.J. 283, 286 (2003) and "implicit protection of autonomy and free choice.").

[10] United States v. Jones, 364 F.Supp.2d 1303 (D.Utah 2005).

[11] Id.

[12] Id.

[13] Id. at 1305.

defendant sought to suppress were his personal e-mail messages intercepted by the informant.[14] Using the information contained in those e-mail messages, the FBI obtained a warrant to search the defendant's computer.[15] Hence, the information found during the warranted search was used against the defendant.[16]

The defendant invoked the Wiretap Act to show that the e-mail messages that had warranted the search had been obtained in violation of the Wiretap Act.[17] The defendant further argued that if the e-mail messages had been unlawfully obtained, the evidence derived from the search warrant should be suppressed.[18]

To support his claim, the defendant compelled discovery to reveal the method in which the informant obtained the e-mail messages.[19] But the court denied defendant's motion to compel discovery of both the identity of the informant witness and the means by which the informant accessed defendant's private email account.[20] Court affirmed the government's refusal to release the identity of the informant – "To protect the safety of that

---

[14] Id.

[15] Id. at 1304.

[16] Id.

[17] Id. at 1305.

[18] Id.

[19] Id.

[20] Id.

informant, this court refused to order disclosure of the information for reasons stated at greater length in the sealed transcript."[21] Thus, the government protected both the informant's identity and the method in which the e-mail messages were obtained.[22]

To remedy the lack of information regarding the informant, this court set out a hypothetical situation:

> This court articulated a "hypothetical" containing the relevant facts to provide Mr. Jones sufficient basis for presenting his claim about the Wiretap Act.[23] According to the hypothetical, Mr. Jones used a computer at a local public library in order to access his email account.[24] After leaving the library computer station, Mr. Jones' email account remained accessible, and a librarian discovered the email messages in Mr. Jones' account.[25] Mr. Jones argues that these facts constitute a violation of the Wiretap Act that should lead to the suppression of evidence.[26]

Now turning to the issue of whether the e-mail messages were obtained unlawfully by the informant, the court examined the history of the Wiretap Act. With the passage of the ECPA, Fourth Amendment protections to cyberspace have evolved to

---

[21] Id.

[22] Id.

[23] Id.

[24] Id.

[25] Id.

[26] Id.

include electronic communications.[27] While ECPA is far from policing and guarding the realm of cyberspace, "ECPA's procedural safeguards concerning stored communications address the gap left by the unclear application of the Fourth Amendment to cyberspace."[28] The courts interpretation of the "ECPA's statutory framework is thus increasingly important to protecting personal privacy in the digital age."[29] Before the ECPA was enacted, the Wiretap Act covered only wire (voice) and oral communications from unlawful interception.[30] But Title I of ECPA, the Wiretap Act, extended the federal wiretap law's protections to electronic communications.[31]

> The Wiretap Act makes it illegal for anyone to "intentionally intercept[] ... any wire, oral, or electronic communication."[32] The court looks to Section 2515 which "provides the sole suppression remedy for unlawfully intercepted communications.[33] 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,

---

[27] Id. at 1306.

[28] Katherine A. Oyama, **E-Mail Privacy After United States v.Councilman: Legislative Options For Amending ECPA**, 1 Berkeley Tech L.J. 499 (2006).

[29] Id. at 503.

[30] Id. at 504.

[31] S. Rep. No. 99-541, at 1, reprinted in 1986 U.S.C.C.A.N. at 1.

[32] 18 **U.S.C.** 2511(1)(a)(2006).
[33] 18 **U.S.C.** § 2515 (2006).

> 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."[34]

While the Wiretap Act was amended to protect the unlawful interception of electronic communications, in the plain language of the statute, the court could not find a suppression remedy for electronic communications already unlawfully intercepted.[35] As a result, the defendant attempted to unsuccessfully argue an abstract "negative implication" theory.[36]

> 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.[37]

Because of the court's disinclination to repeal rules by implication, the court rejected defendant's negative implication theory and interpreted the statute according to the plain meaning of the language.[38] Another theory the defendant tried to

---

[34] Id.

[35] Katherine A. Oyama, **E-Mail Privacy After United States v.Councilman: Legislative Options For Amending ECPA**, 1 Berkeley Tech L.J. 499 (2006).

[36] United States v. Jones, 364 F. Supp. 2d at 1307.

[37] Id. at 1307.

[38] Id.

argue was the possibility that the informant had obtained the e-mail password "by means of an unlawful wire or oral interception" and any information "derived therefrom" is "subject to suppression."[39] Thus, the defendant proposes the theory that the informant had received the information to access the e-mail (such as the password to defendant's e-mail) by oral or wire communications.[40] If this scenario were true, the e-mail messages, as evidence derived from the unlawfully obtained oral or wire communications could qualify under the suppression remedy and be suppressed.[41]

This theory was unconvincing due to the lack of evidence and the specific manner in which the informant must have unlawfully intercepted the wire or oral communication.[42] Using the current definition of wire communications, the government filed an underseal pleading refuting defendant's claim that the e-mail messages were derived from oral or wire communications.[43] Further, the defendant's theory did not avail due to the

[39] Id. at 1309.

[40] Id.

[41] Id.

[42] Id.

[43] Id.

requirement that the oral or wire communications must have been obtained by some mechanical or other type of device.[44]

Had the defendant been able to get around the suppression remedy problem, the defendant could have proposed another theory under the Stored Communications Act, or SCA.[45] However, the defendant did not have cause to invoke the SCA and instead attempted to use the Wiretap Act to suppress the unlawfully obtained e-mail messages.

Consequently, defendant attempts to repeal section 2517 by negative implication and prove that the informant obtained the password through oral or wire communications using an electronic or mechanical device fails. And the defendant loses the case on the finding that the suppression remedy does not cover electronic communications.[46]

III. Analysis

The formal definition of "wire communications" included electronic communications and is probative evidence of the almost identical nature of the two types of communications.[47] The fact that electronic communications had been a type of communication recognized as wire communications is a strong suggestion that the two are related. However, the ECPA recently

---

[44] Id.

[45] 18 **U.S.C.** § 2701 (2000).

[46] Jones, 364 F. Supp. 2d at 1309.

[47] NC

revised the definition of "wire communication" to explicitly exclude electronic communications (instead made a separate categorical definition for electronic communications):

> Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection ... furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.[48]

Without access to information on how the informant unlawfully intercepted the e-mail messages, the defendant's case was greatly debilitated. Thus, the mysterious and non-disclosed nature of the informants' identity and the situation surrounding the interception really made an impact as to the available arguments for the defendant. And the court successfully established a firm guard around the identity of the informant.

Nevertheless, the court focused on the technical language of the Wiretap Act and seemed to lose sight of the main purpose of the Wiretap Act—to protect a citizen's "reasonable expectation of privacy."[49] In the midst of the uncertainty in cyberspace law and the Fourth Amendment, the court, while interpreting the law in the area of privacy, must not neglect

[48] 18 U.S.C. § 2510(1)(2000).

[49] 389 U.S. 347, 353 (1967).

the "reasonable expectation of privacy test" set in Katz v. United States.[50]

In this case, the Supreme Court found that the Fourth Amendment requires law enforcement to obtain a search warrant when monitoring phone calls made from a public telephone booth.[51] In his concurrence in Katz, Justice Harlan articulated the "reasonable expectation of privacy test" for determining whether the Constitution protects an individual's right to privacy from intrusion by the government.[52] The two-pronged test requires that (1) an individual "have exhibited an actual (subjective) expectation of privacy," and (2) "the expectation be one that society is prepared to recognize as [objectively] 'reasonable.'"[53]

IV. Evaluation

As technology develops and e-mail "becomes more commonplace means of communication," it is objectively reasonable for the members of modern-day society to expect that unlawfully obtained e-mail messages will be barred from being used against them in a

[50] 389 U.S. 347, 353 (1967).

[51] Id. at 361.

[52] Id. at 361 (Harlan, J., concurring). See generally, Daniel J. Solove & Marc Rotenberg, Information Privacy Law 21 (2003).

[53] Id. at 361.

criminal or civil trial.[54] Because of the tremendous advancements in technology, more and more people are adopting e-mail into their everyday lives. Therefore, it may be objectively reasonable for members of society to expect that their e-mails will be provided the same degree of protection given to other forms of communications such as wire or oral. For example, many more people are sending out e-mails on a daily basis rather than picking up the phone or sending out faxes.

Yet, due to the uncertainty and open nature of cyberspace, it is undeniable that e-mail is not a very private means of communication. Once a person sends out an e-mail, the sender has risked the possibility that someone other than the intended recipient may get a hold of the e-mail. It can also be thought that the person sending the e-mail has essentially dropped off his personal communication into public space for public eyes.[55]

The ability of people to obtain passwords either through eavesdropping or even through more technologically advance means, such as hacking, has contributed to the numerous instances where people's e-mails have been intercepted by unintended recipients. While the unknown and mysterious nature of cyberspace may give many people a sense of security, in reality, people are mistaken about the level of security. The

---

[54] Robert A. Pikowsky, **Privilege and Confidentiality of Attorney-Client Communication Via E-mail**, 51 Baylor L. Rev. 483 (1999).

[55] Id.

ease with which a person's e-mail may be accessed is evidenced by looking at your own life where you hear of friends and family accessing each other's e-mail accounts.

Consequently, society may be unreasonable in having an expectation of privacy in their e-mail communications. Yet, because e-mail is so commonly used and relied upon by corporations and individuals, e-mail has become almost a necessity to everyday life. The minor differences between e-mail and regular mail should not prevent the law from bestowing the same protections to the realm of cyberspace.

Another interesting point that should be raised is the fact that electronic communications were formally within the definition of wire communications. The almost interchangeable nature of electronic and wire communications should shed some light on why e-mail should be given the same privacy protections given to wire or oral communications. In other words, e-mail should not be treated any different from wire and oral communications.

It is highly arguable that the same protections given to regular mail need to be given to e-mail because people expect the same protections given to regular mail to be given to e-mail. The reasons for these expectations are ingrained in the very nature of e-mail. The fact that the communication is electronic and paperless gives e-mail a uniquely private and protected quality. E-mail is further protected by that fact

that another person may not access your e-mail communication without a password. Thus, in reliance of these protections inherent in e-mail, corporations and individuals alike send out private communications via e-mail on a daily basis.

While the internet and technology is a confusing and unsettled area of law, the court must not neglect the goals of Fourth Amendment privacy protections of "reasonable expectations of privacy."[56] The open and untouchable nature of the internet may thwart the court from affording the same privacy protections to e-mail as it does to mail.

However, regardless of whether a private communication travels through air or cyberspace, the medium of communication should not have an impact on the protection of privacy given by the law. Just as the transition of the law developed during the telephone era and other forms of wire devices, the law should conform to the changing needs of the society. It is evident that e-mail is quickly broadening its reach through America. And people are becoming more and more reliant on e-mail due to the many beneficial features of e-mail such as speed, efficiency, and ease of use. The law should respond to these technological advances because a citizen's expectation of privacy should be the same as to any type of private communication whether it be electronic, oral, or paper.

[56] Katz v. United States, 389 U.S. 347, 353 (1967).

Understandably, this is a controversial issue with strong argument on both sides of the table and courts must continually develop case law with the proper backdrop in mind. As new issues arise and present difficult problems, the courts ought to never lose focus on the goal of the Fourth Amendment – to protect the "reasonable expectation of privacy."[57]

A. Reasons to Find a Constitutional Remedy

Before us now is the issue of whether e-mail is secure enough to support a reasonable expectation of privacy. For example, is e-mail secure enough to sustain the attorney-client privilege and satisfy the attorney's ethical obligation to preserve client confidences?[58]

In the unlikely event that someone other than the intended recipient intercepts e-mail containing a confidential attorney-client communication, does the communication retain its privilege?[59] Has the attorney breached the ethical duty to safeguard confidential communications simply by exchanging

---

[57] U.S. Const. Amend. XIV ("Nor shall any State deprive any person of life, liberty, or property, without due process of law ... .").

[58] Robert A. Polowsky, **Privilege and Confidentiality of Attorney-Client Communication Via E-mail**, 51 Baylor L. Rev. 483 (1999).

[59] Id.

sensitive e-mail with a client?[60] Should attorney disciplinary authorities set out regulations governing the acceptable use of e-mail between attorney and client?[61] These are all crucial questions, an attorney must consider before deciding to rely on the privacy protections afforded to e-mail before sending out privileged information. Just how secure is e-mail? And what should society's expectations be as to the privacy of e-mail? These difficult questions are not answered in this case but are nonetheless pivotal in deciding whether the unlawfully intercepted e-mail messages should have been suppressed under the U.S. Constitution.

Even if the suppression remedy in the Wiretap Act did not cover electronic communications, the court should not have stopped their assessment with the Wiretap Act. A remedy not explicitly contained in a statute does not necessarily mean there is no remedy within the U.S. Constitution. The court's failure to look beyond the plain language of the Wiretap Act's suppression remedy unjustly denied the defendant his privacy protections granted to him within the penumbras of the U.S. Constitution.[62]

The court's desire to give due regard to the legislature by deferring to the plain language of the statute instead of

---

[60] Id.

[61] Id.

[62] Id.

reading into the statute its own interpretation is honorable. Nevertheless, when a particular statute clearly leaves out an expected protection, the court should not turn a blind eye to the deficiency in the statute. It is the courts role to step in and conduct the proper role of judicial review and serve as an appropriate check on the legislative and executive branch.

B. Definitional Similarities Between Wire and Electronic Communications

The similarities between the definition of wire communications and electronic communications in section 2510 indicate that distinguishing the two types of communication is redundant. The almost identical and overlapping nature of wire and electronic communications make it very difficult for even the sophisticated reader to clearly delineate where the differences lie. The definition of wire communications is:

> Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.[63]

The wire communication definition is almost indistinguishable from the definition of electronic communication. Compare the definition of wire communication to the current definition of electronic communications:

[63] 18 **U.S.C.** § 2510(1)(2006).

> "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;[64]

The two definitions both have to do with the transfer of communication by wire. From comparing the two definitions, one can infer that certain types of electronic communications are in essence wire communications because both include transfers by wire. So the confusion and difficulty in figuring out when a transfer by wire is an electronic communication and not wire communication lies in the technical difference between "aural transfers" and "transfers." The reasoning behind legislature to make this distinction is unclear.

There may have been some scientific explanation for the differentiation between an aural transfer and a regular transfer but to the lay person, the separation seems to only cause confusion and redundancy. The definitional similarities evidence the fact that the two areas of communication are

[64] 18 **U.S.C.** 2510(12)(2000).

closely intertwined and should not be separated. The fact that electronic communications transferred over wire are not aural transfers but simply transfers should not create reason to set electronic communications apart from wire communications. Hence, the technical difference between "aural transfers" and "transfers" should not provide reason for separation.

Both the fact that electronic communications had been once part of the definition of wire communications and the fact that the electronic communications had once been under the umbrella of wire communications suggest the unreasonableness in affording unequal privacy protections to both types of communication.

C. Punishing the Perpetrator Without Affording a Remedy to the Victim is Inconsistent

Then the question becomes, what is the purpose behind punishing the perpetrator but denying the victim an adequate remedy for the harm suffered. In this case, the defendant's e-mail was unlawfully obtained and used against him. While the informant unlawfully obtained the e-mails which led to the warrant of a search, the defendant had absolutely no remedy. This seems to open the door for people to hack into other people's e-mails and threaten to turn over information using the protections of police immunity.

Yet the court does not seem concerned with assessing the informants conduct but rather hiding the entire situation under a blanket immunity. Therefore, the defendant is left with a

lost cause. And while the informant could have violated many protections afforded even within the Wiretap Act, the defendant does not currently have a remedy to any of the violations.

Although there have been extensive amendments with the progression of technology and just as much thought put into new cyberspace law, e-mail is still not given the same protections as wire or oral communication.

In this current e-mail age, it is impractical and nonsensical to differentiate between e-mail and other forms of communication. While instant messaging and other forms of electronic communication may not be as widely used as e-mail, this generation of computer users is quickly incorporating "chatting" into their daily lives. And soon instant messaging may be seen as another form of oral communication and be brought in the context of privacy. As instant messaging and other forms of electronic communication become more secure and prevalent in society, the court must address in due time and afford the same privacy protections as needed. But this issue is not within the scope of this comment.

V. Conclusion

The possibility that the suppression remedy's exclusion of electronic communication may be in conflict with the privacy protections found within the "penumbras" of the U.S Constitution. The courts assessment of society's reasonable expectation of privacy in e-mail is an area of law that has been

evolving. But to deny a suppression Remedy and allow unlawfully obtained e-mails to be used against the victim is intrusion into the citizen's constitutionally protected zone of privacy.

Further, this exclusion of electronic communications seems to be out of line with the heavy reliance on the protection of privacy in e-mail by corporations and individuals alike. As the use of e-mail progresses and area of technology advances, the courts should closely assess the reasonable expectations of privacy existing currently in society.