TECHNOTES

# THE WIRETAP STATUTE: A HAVEN FOR HACKERS

**Diana Wilkes***

ABSTRACT

*Voice mail system (VMS) technology, a relatively new computer application, is becoming common in larger business offices. As with other electronic information networks,[1] System Operators[2] are at constant risk of invasion by computer hackers.[3] System Operators expend considerable time and money in unsuccessful efforts to identify and apprehend these invaders, efforts which are hampered by cumbersome communications equipment, limited resources, and an inadequate Wiretap Statute. Law enforcement's resources to battle hackers are mainly limited to interception and trap-and-trace devices.[4] The ambiguous Wiretap Statute dictates the manner and circumstances under which law enforcement may employ these devices. This article argues that the Fourth Amendment[5] must accommodate a Wiretap Statute that provides for more efficient and effective law enforcement tools in the face of everchanging technology.*

## I. THE VMS PROBLEM

### A. The Voice Mail System

A VMS is a computerized telephone message system.[6] Users have individual VMS mailbox numbers to receive messages. Hackers contact the VMS through

---

*J.D., Arizona State University, 1990. Member of the Arizona Bar.

[1]This same analysis would also apply to computer fraud generally.

[2]A System Operator, usually a business, leases or owns the VMS computer system as a telecommunications industry customer.

[3]The VMS hacker may be a computer hacker or a "phone freak" (a hacker who manually dials numbers on the telephone keypad).

[4]A trap-and-trace device traces a call from the destination, through switching equipment to the point of origin, produces a printout showing the time of the call and the originating telephone number and, when matched with VMS information, identifies a VMS hacker.

[5]U.S. CONST. amend. IV.

[6]A VMS generally has three levels of User access: (1) the Caller dials the System Operator telephone number and hears a general greeting, (2) the Caller leaves a message for a particular

the System Operator's "800" telephone line,[7] through telephone company switching equipment,[8] or by using stolen telephone credit card numbers. The hacker gains access to the VMS by using either "shared"[9] or "hacked"[10] access codes. VMS hackers clog business telephone lines[11] with illegal calls, contributing to the $500 million per year in general communication fraud loss.[12]

Losses attributable to VMS hackers increase geometrically as the size of the hacker group increases.[13] Hackers access a VMS at various levels: (1) the "User Hacker" assigns herself a previously unassigned or inactive mailbox; (2) the "Caller Hacker" leaves messages for the User Hacker; and (3) the "System Hacker" invades the VMS at the System Manager level. VMS hackers use "handles"[14] to refer to themselves and rely on the VMS's destructive update feature[15] to avoid detection. The System Hacker can destroy evidence of any hacker's presence, place an offensive general greeting on the VMS,[16] or shut down the VMS, crippling a System Operator's business until the VMS program is reinstalled.

---

User; and (3) the User enters a user password to retrieve a message. A VMS has also at least one level of System Manager access that is necessary to maintain the system at the highest level, allowing the System manager to "look at" messages in a VMS mailbox, to delete messages, and to change the greeting.

[7]Generally a System Operator maintains "800" telephone lines to provide toll-free access to customers and employees.

[8]The VMS hacker may also assign himself a telephone number that does not exist in any physical location. Charges for calls from these telephones are not referred to the billing system.

[9]VMS hackers often share codes by posting them in other VMS mailboxes or on illegal computer bulletin boards.

[10]"Hacking" access codes involves trying a series of numbers generally in sequential order, until the VMS hacker discovers a valid combination. The manual process is laborious and time-consuming, but a computerized automatic dialer connected to telephone lines through a modem facilitates the process.

[11]In some cases, a System Operator's failure to utilize security measures assists the hacker's VMS access; even security measures aimed at prevention and detection do not prevent a VMS from being hacked by a persistent or lucky VMS hacker. Even if a VMS System Operator fails to use adequate security measures, the VMS hacker is as culpable as a burglar entering through an unlocked door. The wrongdoer should be punished, not the person failing to prevent the wrong. "Effective management of security on mechanized systems requires an astute employee body." Telephone interview with Frocine Adams, Executive Director of Security, US West Communications (Feb. 16, 1990).

[12]Calculated at an annual rate of 1% of a $50 billion industry; this estimate includes losses to both communication and private industry. Telephone interview with Rami Abuhamdeh, Executive Director, Communications Fraud Control Association (Feb. 16, 1990).

[13]VMS hackers travel in packs. Each VMS hacker may have an assigned mailbox, with each VMS hacker receiving messages and calling others. For example, 20 VMS hackers can place 400 telephone calls a day if each calls each of the other 19 once a day and checks an assigned mailbox once a day for messages. These calls can total 12,000 per month or one telephone call every 3.6 minutes in a 24-hour period. The VMS hackers strike, stay as long as they feel safe, then move to another VMS. Telephone interview with Toni Ames, Security Manager, US West (Feb. 15, 1990).

[14]Cross-referenced lists attempting to match VMS hacker handles (nicknames) with given names and telephone numbers become useless when the VMS hacker changes his handle to avoid detection. Telephone interview with Law Enforcement Agent (requested anonymity pending final disposition of case), United States Secret Service, Phoenix, Arizona (Feb. 16, 1990).

[15]Retrieving a message removes it from the computer memory.

[16]T. Ames, *supra* note 13.

The VMS hacker's ability to instantly destroy evidence and/or exit the VMS illustrates the exigent circumstances involved in investigating, apprehending, and prosecuting these elusive criminals. For example, the System Manager discovers that a previously unassigned VMS mailbox has suddenly sprung alive with activity[17] and contacts the appropriate law enforcement agency. The investigating officers must apply for a wiretap order to intercept future hacker communications. The process is complicated and time-consuming,[18] involving interviews with experts and possibly a lengthy investigation. Before the application process is complete, the VMS hackers may move to a new VMS and wreak havoc on another System Operator's business. An inadequate Wiretap Statute[19] facilitates the VMS hacker's mischievous mission.

## B. The Wiretap Statute

The Wiretap Statute imposes criminal and civil liability for intercepting a wire communication in violation of its provisions. Although intended to balance individual privacy expectations and law enforcement needs, the statute inadequately protects innocent System Operators' rights. The procedures mandated by the statute are too cumbersome to be effective in the VMS hacker situation. Although law enforcement may learn inadvertently discovered communications[20] or those divulged with the consent of the originator, addressee, or intended recipient,[21] the statute does not define these and other key terms, a problem which hinders law enforcement and helps the VMS hacker.[22] System Operators and the communications industry are understandably reluctant to cooperate with law enforcement agencies when the statute does not clearly dictate who has the right to divulge VMS communications or consent to a wiretap.

A wiretap order will issue only upon a showing of probable cause[23] and necessity.[24] An applicant may face an even greater obstacle in the statute's provision for challenging a wiretap order. Any named target or intercepted user[25]

---

[17]In reality, within a short time period, VMS hackers would activate several mailboxes, each showing a flurry of activity.

[18]In practical terms, a 10-day delay could represent 4,000 illegitimate telephone calls for a group of twenty VMS hackers. *See supra* note 13.

[19]The Wire and Electronic Communications Interception and Interception of Oral Communications Act, 18 U.S.C. §§ 2510-2521 (1986). *See* S. REP. No. 541, 99th Cong., 2d Sess., pt. III at 5 (1986).

[20]18 U.S.C. § 2511(3)(b)(iv).

[21]18 U.S.C. § 2511(3)(b)(ii).

[22]The statute fails to state whether the VMS System Operator is a party to the conversation, an addressee or an intended recipient; whether inadvertent discovery means discovery through the monthly telephone statement, or only during system maintenance; and whether inadvertent discovery includes only the first or all subsequent communications.

[23]18 U.S.C. § 2518(3).

[24]18 U.S.C. § 2518(3)(c); *see also* United States v. Marquez, 686 F. Supp. 1354, 1364 (N.D. Ill. 1988) (The necessity showing is required to assure that, if traditional investigative techniques are adequate, law enforcement does not resort to the intrusive investigative tool, the wiretap).

[25]18 U.S.C. § 2510(11).

(even the hacker, who by definition is illegitimately using the VMS) may challenge the validity of an order for specified reasons.[26]

Moreover, under the current Wiretap Statute, the VMS hacker could potentially pursue a civil cause of action against one who "unlawfully" intercepted his telephone call. Even worse, the person intercepting an illegal VMS hacker call risks criminal liability: the innocent System Operator could actually be prosecuted for confronting the invading hacker within the VMS, with the hacker appearing as the prosecution's main witness. The rights of a criminal defendant deserve protection but should not be paramount to those of the victim.[27]

VMS crimes differ from those addressed in the current wiretap Statute, which is mainly concerned with offenses such as gambling, organized crime, and drugs.[28] Congress likely did not consider the VMS hacker when revising the current wiretap statute in 1986 as the problem was not yet apparent.[29] Consequently, the statute does not provide for an expedited application process, a critical tool in exigent circumstances where a criminal can strike, destroy evidence, and disappear with the speed of an electronic signal.[30]

The only authorized use of a VMS mailbox occurs after it is assigned, so the very existence of any activity on an unassigned VMS mailbox is presumptively illegitimate.[31] Therefore, every call to an unassigned VMS mailbox will be germane to VMS hacker prosecution.[32] A VMS wiretap does not intercept other users' calls or legitimate calls of the VMS hacker, as would a wiretap on a home or business telephone. Unlike a regular wiretap, the VMS wiretap will not impinge on any legitimate privacy interest. These differences call for rethinking the scope and application of appropriate law enforcement tools.

---

[26]18 U.S.C. § 2510(10)(a)(i)–(iii).

[27]C-Span, U.S. House, Judiciary Subcommittee on Criminal Justice Concerning Computer Viruses, Nov. 8, 1989 (C-Span Network television broadcast, Dec. 24, 1989) (testimony of Carolyn Conn, Co-Chairman, Government Relations Committee, Electronic Data Processing Auditors Association), 135 CONG. REC. 1322 (daily ed. Nov. 8, 1989).

[28]*See generally* S. REP. No. 541, 99th Cong. (1986).

[29]Telephone Interview with Gail H. Thackeray, Assistant Attorney General, Arizona Attorney General's Office, Feb. 8, 1990.

[30]Exigent circumstances except a search from the Fourth Amendment search warrant requirement when the suspect is fleeing or evidence is in danger of being destroyed. *See, e.g.*, United States v. Irizarry, 673 F.2d 554, 557 (1st Cir. 1982). Although the nature of VMS fraud would lend itself to arguing an exigent circumstance exception on which to base the EEWO, this article does not take that position because of the nature of the technology and the status of wiretap law. A VMS hacker using a telephone to access the VMS computer is not analogous to a fleeing felon. A fleeing felon can be chased. Once the telephone connection is broken, a VMS hacker has severed any "visual" contact necessary to pursue him or her. Also, destruction of evidence may allow law enforcement time to intercede and prevent the destruction. Destruction of evidence of VMS hackers on a VMS is instanteous—once appropriate commands are entered, the evidence is gone. Only if a telephone could be tapped without any order, a drastic measure for financial loss, would this argument be applicable.

[31]Even an employee could be a VMS hacker if the employee is not authorized to use an unassigned VMS mailbox.

[32]Interception of a legitimate call is limited to the instance of a legitimate caller dialing the wrong VMS.

## II. A PARTIAL SOLUTION

A wiretap is especially appropriate where the telephone is routinely used in furtherance of a crime.[33] The drug addict calls his source; the gambler calls his bookie; the syndicate boss calls his henchmen to give them instructions.[34] Each uses the telephone as a convenient but unnecessary instrument to further the crime.[35]

*A fortiori*, then, a wiretap is appropriate if the telephone is the instrumentality of crime. The VMS, a telephone system component, is the direct target of the VMS hacker. The VMS hacker's crime demonstrates his intent: he dials into the VMS, hacks out codes, records or retrieves messages, or compromises the VMS. He uses the telephone as the instrumentality of, rather than in furtherance of, his crime. The innocent victim of VMS vandalism is often unaware of the crime or even of the hacker's presence.

The VMS hacker should have no expectation of privacy as against a VMS victim.[36] The VMS hacker knowingly "trespasses" into the VMS and steals thousands of dollars worth of long distance calls from the innocent System Operator. Nevertheless, legitimate privacy concerns demand that some requirement for a wiretap order be imposed, notwithstanding law enforcement efficiency[37] and simplicity[38] concerns. The foregoing discussion suggests two statutory amendments: (1) an Electronic Emergency Wiretap Order (EEWO) would be the perfect tool to balance the competing interests at stake; and (2) alternatively or in tandem, Congress could amend the Wiretap Statute to deny to one not legitimately on the VMS automatic standing to challenge interception of the communication.[39]

---

[33]United States v. Young, 822 F.2d 1234, 1237 (2d Cir. 1987) (citing United States v. Steinberg, 525 F.2d 1126, 1130 (2d Cir. 1975), *cert. denied*, 425 U.S. 971 (1976)).

[34]The Wiretap Statute provides a "roving wiretap" to deal with targets who frequently change telephones to avoid interception of their communication. 18 U.S.C. § 2518(11); *see generally* S. REP. No. 541, 99th Cong., pt. III at 5 (1986). This provision is inadequate in the VMS situation because the roving wiretap was intended to be used against someone using different originating telephones, rather than different destination points targeted by the VMS hacker.

[35]*See generally* S. REP. No. 541, 99th Cong. (1986).

[36]"In practice, current statutes actually appear to protect the rights of the intruder. *Persons attacking the integrity of computer systems or communications networks should have no expectation of privacy as against their victims*. . . . It must be clear that the owner of the network or the computer system has authority to investigate and turn over to law enforcement officials any evidence of intruder activity." C-Span, U.S. House, Judiciary Subcommittee on Criminal Justice Concerning Computer Viruses, Nov. 8, 1989 (C-Span Network television broadcast, Dec. 24, 1989) (testimony of Carolyn Conn, Co-Chairman, Government Relations Committee, Electronic Data Processing Auditors Association), 135 CONG. REC. 1322 (daily ed. Nov. 8, 1989) (emphasis added).

[37]"[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment." Mincey v. Arizona, 437 U.S. 385, 393 (1978).

[38]"The investigation of crime would always be simplified if warrants were unnecessary. But the Fourth Amendment reflects the view of those who wrote the Bill of Rights that . . . privacy . . . may not be totally sacrificed in the name of maximum simplicity in enforcement of criminal law." Mincey, 437 U.S. 385 at 393.

[39]As a third alternative, the term "party to the conversation" could be redefined to include the owner of the equipment. Such an amendment would allow the System Operator to consent to the interception of the communication. 18 U.S.C. § 2511(2)(c). Although this approach offers the

## A. Electronic Emergency Wiretap Order

An EEWO, limited to the scope justified by VMS exigencies,[40] would address the exceptional VMS hacker circumstances which make the procedure for a regular wiretap order impracticable. The EEWO would be limited to a ten-day period with only one renewal based on a showing of good cause. This ten-day period would allow law enforcement adequate time to prepare an application, if necessary, for a regular wiretap order. The EEWO differs from an order authorizing a wiretap on the VMS hacker's home telephone. The hacker has a legitimate interest in communications on his own telephone. A wiretap order under the current statute is, and should be, required to tap the hacker's telephone. However, an EEWO would authorize a tap on an unassigned VMS mailbox, not the hacker's home telephone, with the System Operator's consent.

The EEWO would issue based on an application verifying that activity on a previously unassigned VMS mailbox is unauthorized so anyone accessing that mailbox is per se a VMS hacker and not legitimately on the VMS.[41] Until VMS hackers are regularly and successfully prosecuted, they will continue "plying [their] trade."[42] Only when efficient law enforcement and systematic prosecution is a reality can we expect to reduce the ranks of VMS hackers and the losses they impose.

"[A regular wiretap order] requirement is not appropriate when 'the burden of obtaining [the order] is likely to frustrate the governmental purpose behind the search.' "[43] The need for a law enforcement tool to respond swiftly to an electronic emergency must be balanced against individual privacy interests.[44] At issue here are the VMS hackers' privacy rights balanced against the government's need for effective measures to protect VMS fraud victims. The critical factors are the "nature of the intrusion and governmental interest."[45] In the VMS hacker situation, the intrusion involves equipment not belonging to, but being invaded by, the hacker.

The wiretap statute protects privacy rights by interposing a detached and neutral magistrate between the law enforcement officer "engaged in the often

---

simplest solution, the amendment (1) would provide the least amount of protection for the VMS Hacker; (2) may allow the System Operator to intercept other than illegitimate calls; and (3) may be more difficult to restrict to VMS hacker or computer fraud applications.

[40]Florida v. Royer, 460 U.S. 491, 500 (1983).

[41]While boilerplate language is inappropriate, a *brief* explanation of the circumstances would be adequate. In addition, if the VMS mailbox were previously assigned, a copy of notice to, or consent of, the authorized user is attached to the affidavit.

[42]Jones v. United States, 362 U.S. 257, 267 (1960).

[43]O'Connor v. Ortega, 480 U.S. 709, 720 (1987).

[44]*Id.* at 719.

[45]A determination of the standard of reasonableness applicable to a particular class of searches requires "balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." United States v. Place, 462 U.S. 696, 703 (1983).

competitive enterprise of ferreting out crime''[46] and the target. To justify a lower standard of probable cause, the suggested EEWO procedure would apply a compelling need standard[47] rather than the lower standard of need required for a regular wiretap order. However, although based on a lower standard of probable cause, the EEWO does not provide an easy way for law enforcement to circumvent constitutional and statutory protections. Rather, the EEWO provides a narrowly tailored means of investigating a specific type of criminal activity for which there is no current effective procedure.

Magistrates will have less information to judge the validity of the application, so they may be less willing to issue an EEWO. Therefore, the statutory amendment should mandate an EEWO if the requisite factors are present. The amended statute should also include an exclusionary provision, with a good faith exception, narrowly tailored to deter inappropriate use of an emergency wiretap, with trumped-up circumstances.

## B. Fourth Amendment Justification for an Electronic Emergency Wiretap Order

An analysis of the Fourth Amendment validity of an EEWO is complicated by the difficult question of precisely who owns the communication at issue in VMS hacking. As a relatively new technology, Voice Mail Systems illustrate the now familiar lag time between technological advancements and the development of adequate legal protection or regulation. Fortunately, Fourth Amendment law in general wiretapping, electronic surveillance, and search warrant areas provides a strong basis for the EEWO.

The Fourth Amendment protects against unreasonable searches and seizures and applies to ''conversation.''[48] Electronic surveillance is a ''search'' and capturing a conversation is a ''seizure.'' Interception[49] is rarely given judicial sanction if law enforcement bypasses the probable cause determination by an independent and neutral magistrate.[50] Courts consistently apply search warrant principles to electronic surveillance,[51] including the concept of reasonable

---

[46]Mincey, 437 U.S. at 395 (*quoting* Johnson v. United States, 333 U.S. 10, 13-14 (1948)).

[47]*Id.* at 393-94; O'Connor, 480 U.S. 709.

[48]*See* Berger v. New York, 388 U.S. 41, 51 (1967); *see also* S. REP. No. 541, 99th Cong., 2d Sess., pt. III at 5 (1986).

[49]Interception is the search and seizure of a conversation.

[50]United States v. Mankani, 738 F.2d 538, 543 (2d Cir. 1984).

[51]*See, e.g.*, United States v. Leisure, 844 F.2d 1347, 1354 (8th Cir.), *cert. denied*, 488 U.S. 932 (1988) (practical and common sense approach in determining sufficiency of wiretap affidavits); United States v. Townsley, 843 F.2d 1070 (8th Cir.), *aff'd in part, vac'd and rem'd on other grounds*, 856 F.2d 1189 (8th Cir. 1988) (wiretap probable cause determination in wiretap affidavit no different than that for search warrant affidavit—totality of circumstances applies); United States v. Aguirre, 839 F.2d 854, 858 (1st Cir. 1988) (totality of the circumstances); United States v. Ippolito, 774 F.2d 1482, 1484-86 (9th Cir. 1985) (practical and common sense approach; *Franks* determination (citing Franks v. Delaware, 438 U.S. 154 (1978)); United States v. Torres,

or legitimate privacy expectations.[52] The hacker has no such privacy expectation where she abandons her communication on the VMS, discloses that communication to a third party (the System Operator), and/or impliedly consents to the recording of her voice communication by leaving a message on the VMS.

### 1. *The VMS Hacker Abandons the Communication Left on the VMS*[53]

Warrantless searches of abandoned property do not violate a defendant's Fourth Amendment rights.[54] Voluntary[55] abandonment of or intent[56] to abandon the property, based on all relevant facts and circumstances,[57] negates both the subjective and the objective expectation of privacy.[58] Courts determine whether property is abandoned based on the totality of the circumstances, emphasizing two factors: denial of ownership and relinquishment of the property.[59]

*Denial of Ownership*. The Ninth Circuit ruled a defendant abandoned his carry-on luggage where he denied ownership and left it on board the airplane.[60] When the hacker leaves a message on the VMS using a handle (or code name), he disclaims ownership. The hacker handle provides the same anonymity a traveler has and the hacker knows he cannot retrieve, change, or in any other way access the message. By analogy, the hacker leaves the message "on board" the VMS.

*Relinquishment of the Property*. A VMS hacker intends to have his voice message recorded. The hacker releases the message to a third party (another unauthorized User Hacker, the System Operator or System Manager) and "physically relinquish[es] control"[61] of the message, thereby losing any expectation of privacy in the communication.[62] After the VMS hacker abandons a communication, the VMS System Operator should be able to intercept, disclose or use[63] that communication to detect and prosecute VMS hackers in the invading group without fear of criminal or civil liability.

---

751 F.2d 875 (7th Cir. 1984), *cert. denied sub nom.* Rodriguez v. United States, 470 U.S. 1087 (1985) (televised surveillance); United States v. Tehfe, 722 F.2d 1114, 1118 (3d Cir. 1983), *cert. denied sub nom.* Sanchez v. United States, 466 U.S. 904 (1984); United States v. Forte, 684 F. Supp. 1288, 1290 (E.D. Pa. 1988) (totality of the circumstances) (citing Illinois v. Gates, 462 U.S. 213, 235 (1983)).

[52]The Supreme Court has used "the words 'reasonable' and 'legitimate' interchangeably." California v. Ciraolo, 476 U.S. 207, 219 n. 4 (1986) (Powell, J., dissenting).

[53]United States v. Knox, 839 F.2d 285, 293 (6th Cir. 1988), *cert. denied*, 490 U.S. 1019 (1989).

[54]*See, e.g.*, United States v. Brady, 842 F.2d 1313, 1315 (D.C. Cir. 1988) (citing Abel v. United States, 362 U.S. 217, 241 (1960) ).

[55]*See, e.g.*, Brady, 842 U.S. at 1316.

[56]United States v. Sylvester, 848 F.2d 520, 525 (5th Cir. 1988).

[57]*Id.*

[58]*See* United States v. McBean, 861 F.2d 1570, 1574 (11th Cir. 1988).

[59]*See, e.g.*, United States v. Nordling, 804 F.2d 1466, 1469 (9th Cir. 1986).

[60]*Id.* at 1469–70.

[61]*Id.*, at 1470.

[62]*See* § II.A.3 relating to disclosure of communications to third parties.

[63]18 U.S.C. § 2511(1).

### 2. *The VMS Hacker Impliedly Consents to the Recording of His Voice Communication*

Searches based on a party's consent are excepted from Fourth Amendment warrant and probable cause requirements.[64] Whether the VMS hacker has "impliedly" consented to the recording of his voice communication is a factual determination.[65] The purpose of a VMS is to record and retrieve messages from callers; the very nature of the hacker's offense indicates his implied consent, and indeed his intent, to have his voice recorded. The VMS hacker purposely dials into the VMS to record his voice communication. He knows that the communication will be recorded. The deliberate, intentional act of the VMS hacker should satisfy any voluntariness test. The VMS hacker clearly has no claim of duress or coercion.

In these circumstances, the third-party consent of the System Operator suffices to authorize a search and seizure, even assuming the hacker has an "ownership" interest in the message. For third-party consent to be valid, the consenting party must have (1) access to the area and (2) a substantial interest in or common authority over the property.[66] The System Operator easily meets both tests.

Such consent is not grounded in principles of property law[67] but in the VMS hacker's assumption of the risk that the System Operator will consent. The Sixth Circuit ruled that where a defendant stored goods in a warehouse, he bore the risk that the warehouseman would consent to a search of the premises and the resulting exposure of goods.[68] Likewise, the VMS hacker bears the risk that the System Operator will consent to a search of the VMS (the premises) and the resulting exposure of the recorded communication (the goods).

A VMS hacker is also analogous to the drug dealer who intends to intercept a package sent through a common carrier before it reaches a third party addressee.[69] The Fourth Circuit ruled that, in this situation, the president of the corporate addressee had authority to open the package and could turn it over to law enforcement.[70] By analogy, the VMS hacker dials through a common carrier's equipment to the VMS addressee and leaves a message. The User Hacker (the intended recipient and interceptor of the communication) plans to remove

---

[64] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

[65] *See id.* at 224, 227, 234.

[66] "A third-party consent is a valid authorization to search, absent a warrant, if the consenting party has both access to the area and either substantial interest in or common authority over the property." United States v. Falcon, 766 F.2d 1469, 1474 (10th Cir. 1985).

[67] "Such consent does not depend upon the law of property but, rather, is premised upon the recognition that one who subjects his property to the joint or exclusive control of another assumes the risk that consent will be granted by the other to a search of the property." *Id.* at 1474.

[68] United States v. Solomine, 536 F.2d 703, 707–708 (6th Cir. 1976), *vac'd, rem'd for sentencing, cert. denied*, 429 U.S. 990 (1977); *but see* Stoner v. California, 376 U.S. 483 (1964) (search of hotel room, although conducted with clerk's consent, was unlawful).

[69] United States v. Givens, 733 F.2d 339, 340–41 (4th Cir. 1984).

[70] *Id.*

the communication from the VMS. The VMS System Manager is generally authorized to remove voice communications from the VMS and should have the right to turn that communication over to law enforcement even if discovery was not inadvertent.

### 3. *The VMS Hacker Has Disclosed the Communication to a Third Party*

The Caller Hacker knows and intends that his communication is being recorded when he leaves that communication with the third party VMS System Operator. Therefore, he assumes the risk that his message will be intercepted and referred to law enforcement.[71] The hacker should not be able to challenge a search warrant by vicariously asserting the rights of the third party[72] recipient of the communication. A party who communicates information has no privacy expectation even where the communication is on a confidential basis.[73] "When you pick up that phone and talk, you can't trust nobody, nohow, nowhere!"[74] Privacy expectations lie with the VMS System Operator, not with the hacker who intended and arranged to have his communication recorded and who deliberately released his communication to a third party.[75]

## C. Standing to Challenge the Wiretap Order

The second suggested amendment to the Wiretap Statute would deny the VMS hacker standing to challenge the EEWO because the hacker is illegitmately using the VMS. Although statutory standing protects important privacy interests,[76] it provides a haven for hackers and burdens law enforcement. With no reasonable expectation of privacy in the area searched, the hacker's Fourth Amendment rights are not implicated.[77] Absent a valid Fourth Amendment claim, the hacker should not have standing to challenge the EEWO.[78] However, under the current Wiretap Statute, the VMS hacker has just that—if his conver-

---

[71] In United States v. Jacobsen, 466 U.S. 109, 117 (1984), the Supreme Court stated:

> [W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information. . . . The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.

[72] United States v. Kinsey, 843 F.2d 383, 389 (9th Cir. 1988).

[73] Securities & Exch. Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984).

[74] United States v. Felton 753 F.2d 256, 260 (3d Cir. 1985).

[75] "[W]here one party to a conversation records it, the expectation of privacy in the recording rests with the possessor of the recording and not the other parties to the conversation." United States v. Wright, 826 F.2d 938, 945 (10th Cir. 1987).

[76] *See generally* S. REP. No. 541, 99th Cong. (1986).

[77] *See, e.g.*, Sylvester, 848 F.2d at 524.

[78] *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 131-34 (1978).

sation is intercepted, he has standing[79] to challenge the wiretap without establishing a reasonable expectation of privacy.[80] A statutory amendment denying standing to those using communications equipment illegitmately would remedy this problem. To establish the legitimate expectation necessary to confer standing to challenge an EEWO, a VMS hacker would be required to show (a) that he had a subjective expectation of privacy[81] and (b) that his subjective expectation of privacy is one that society is prepared to recognize.[82]

A subjective expectation of privacy is present where the VMS hacker "thought of the place . . . as a private one, and treated it as such."[83] Without doubt, the VMS hacker subjectively expects, or at least hopes, that the communication he places on the System Operator's VMS will remain private. The User Hacker appropriates an unassigned VMS mailbox and assigns a secret password. The Caller Hacker calls a specific mailbox. Although these efforts indicate an attempt by the User Hacker to maintain privacy, when designed to conceal criminal activity they demonstrate "that the expectation of privacy was [not] *legitimate* in the sense of the Fourth Amendment."[84] Simply putting up barriers, such as the VMS mailbox password, to avoid detection is not the type of privacy expectation that society is willing to recognize.[85] The VMS hacker may not claim a legitimate expectation of privacy simply because he has a subjective expectation of not being discovered.[86] A VMS hacker's subjective expectation of privacy in a recorded communication left accessible to others on the System Operator's VMS is "objectively unreasonable."[87]

A legitimate expectation of privacy must find its basis outside the Fourth Amendment[88] in factors society recognizes as legitimate. Society has long recognized that legitimate presence on the premises is an important factor in finding a reasonable expectation of privacy.[89] Other factors in determining whether

---

[79]18 U.S.C. § 2518(10)(a).

[80]In a search warrant situation, if the defendant were not on the premises legitimately, he would lack standing. *See, e.g.*, Rakas, 439 U.S. 128.

[81]California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979) ).

[82]*Id.*

[83]*See, e.g., United States v. Aguirre*, 839 F.2d 854, 857 (1st Cir. 1988) (the court looked "to whether or not the individual thought of the place (or the article) as a private one, and treated it as such"); *but see* United States v. Dass, 849 F.2d 414, 415 (9th Cir. 1988) ("Fourth Amendment protection is not premised upon the nature of the item ultimately discovered, but upon the seizure itself").

[84]Oliver v. United States, 466 U.S. 170, 182 (1984) (The defendant grew marijuana on secluded land, erected fences, and posted "No Trespassing" signs in an effort to conceal his illegal crop).

[85]*Id.*

[86]United States v. Whaley, 779 F.2d 585, 590–91 (11th Cir. 1986) (*en banc*), *cert. denied*, 479 U.S. 1055 (1987).

[87]*Id.*

[88]United States v. Vicknair, 610 F.2d 372, 379 (5th Cir. 1980), *cert. denied*, 449 U.S. 823 (1980) (citing Rakas, 439 U.S. at 143, n. 12).

[89]*See generally* Rakas, 439 U.S. at 139–49.

a defendant has a legitimate privacy expectation include ownership or possessory rights,[90] exclusive control,[91] the right to exclude others,[92] unencumbered access,[93] permission to enter the premises in the absence of the rightful possessor,[94] the type of connection with the place searched,[95] and the prior use of the area searched or property seized.[96]

Mere presence[97] or wrongful presence[98] "cannot invoke the privacy of the premises searched."[99] The courts have held the defendant has no reasonable expectations of privacy in a stolen automobile,[100] in a motel room after the rental period has expired,[101] or in a room that he never checked into or for which

---

[90]*See, e.g.*, United States v. Zabalaga, 834 F.2d 1062, 1065 (D.C. Cir. 1987) (defendant did not have a legitimate expectation of privacy where he could not show that he owned or leased the automobile searched, nor that he had the permission of the owner to drive the auto); United States v. Martinez, 808 F.2d 1050 (5th Cir.), *cert. denied*, 481 U.S. 1032 (1987) (as the lawful possessor of the automobile searched by law enforcement, the defendant had standing to contest search); United States v. Wright, 826 F.2d 938, 944 (10th Cir. 1987) (defendants had neither ownership nor possessory interest in cassette tape and documents seized during search of a business which was used as a front to obtain funds on a pretense); *but see* United States v. Medina-Verdugo, 637 F.2d 649, 652 (9th Cir. 1980) ("ownership is but one factor to consider in determining whether one has a reasonable expectation of privacy." The court held that defendant, who, in order to avoid detection of drug possession at border, gave packet to girlfriend to place in her purse, lacked a privacy interest even though he later claimed an ownership interest); United States v. Nadler, 698 F.2d 995, 999 (9th Cir. 1983) ("while the defendant's possessory interests in either the premises or the seized goods are relevant, they are not dispositive"); United States v. Rahme, 813 F.2d 31, 34 (2d Cir. 1987) (neither ownership nor possession, in themselves, are sufficient to establish a legitimate expectation of privacy; other factors must be examined).

[91]United States v. Horawitz, 806 F.2d 1222, 1225 (4th Cir. 1986) (control, for Fourth Amendment purposes, is "measured by physical presence in, or access to the area to be searched, . . . and by ability to exclude others. . . . Although an individual need not maintain absolute personal control (exclusive use) over an area to support his expectations of privacy, 'occasional presence, without any right to exclude others, is not enough' ").

[92]Haydel, 649 F.2d at 1155 (5th Cir. 1981) ("Other factors [besides property ownership] to be weighed include whether the defendant has a possessory interest in the thing seized or the place searched, whether he has the right to exclude others from that place, whether he has exhibited a subjective expectation that it would remain free from governmental invasion, whether he took normal precautions to maintain his privacy and whether he was legitimately on the premises).

[93]United States v. Wiley, 847 F.2d 480, 481 (8th Cir. 1988).

[94]*Id.*

[95]U.S. v. Mankani, 738 F.2d 538, 544–45 (2d Cir. 1984).

[96]United States v. Gomez, 770 F.2d 254 (1st Cir. 1985). Connection with or prior use of area searched or property seized could include, *inter alia*, keeping possessions on the premises or receiving mail at the premises. Wiley, 847 F.2d at 481.

[97]United States v. Kinsey, 843 F.2d 383, 390 (9th Cir. 1988) ("mere presence in the motel room of another is not enough [to confer standing]"); United States v. Irizarry, 673 F.2d 554, 556 (1st Cir. 1982) (where defendant, present in a hotel room registered to a co-defendant, offered no evidence of any personal interest in the room beyond being "merely present," and in fact sought to deny any connection with the room and its contents, evidence seized may be admitted).

[98]Rakas, 439 U.S. 128.

[99]*Id.* at 141 n.9 (1978) (quoting Jones v. United States, 362 U.S. 257, 267 (1960)).

[100]*See, e.g.*, Rakas, 439 U.S. at 141–45.

[101]*See, e.g.*, United States v. Ramirez, 810 F.2d 1338, 1341 (5th Cir.), *cert. denied*, 484 U.S. 844 (1987) (citing United States v. Jackson, 585 F.2d 653, 658 (4th Cir. 1978); *accord* United States v. Larson, 760 F.2d 852 (8th Cir. 1985).

he never paid.[102] Finally, a burglar's presence in a summer cabin off-season is "wrongful."[103]

An authorized customer of the System Operator,[104] legitimately on the VMS, would have not only a reasonable expectation of privacy but would fall within the class of persons Congress intended to protect by providing statutory standing to challenge a wiretap order.[105] When Mr. Katz stepped into the telephone booth where the Supreme Court found an expectation of privacy,[106] he fulfilled his portion of a contract with the telephone company. He deposited a dime in the telephone to pay for his telephone call. At that moment, he and the telephone company entered into a contract wherein the company agreed to provide him with the telephone service for the duration of the call. Mr. Katz had a reasonable expectation of privacy, largely because he was legitimately on the premises.

In contrast, the VMS hacker, using free long distance telephone service, invades the System Operator's VMS to leave and check messages, possibly causing the System Operator to lose customers. The VMS hacker is not legitimately on the premises, has no reasonable expectation of privacy, and should lack standing to challenge any wiretap.

## III. CONCLUSION

The Electronic Emergency Wiretap Order procedure and underlying policy are merely starting points for dealing with the VMS hacker problem which is here to stay. With each new wave of technology, a new brand of criminal appears on the horizon. Congress should emphasize "individual accountability as the cornerstone of computer ethics."[107] As VMS hackers impose losses on unsuspecting companies, law enforcement must have an effective tool to detect and prosecute these smug members of the electronic subculture. Yet, in a delicate balance, Congress must maintain protection of United States citizens' privacy rights.

---

[102] United States v. Carter, 854 F.2d 1102, 1105–06 (8th Cir. 1988).

[103] Rakas, 439 U.S. at 143 n.12 (*quoting* Jones, 362 U.S. at 267).

[104] As with other overhead costs, the cost for VMS fraud is an overhead cost which becomes a factor in pricing the System Operator's product or service.

[105] 18 U.S.C. § 2518(10); *see generally* S. REP. No. 541.

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

[107] C-Span, U.S. House, Judiciary Subcommittee on Criminal Justice Concerning Computer Viruses, Nov. 8, 1989 (C-Span Network television broadcast, Dec. 24, 1989) 135 Cong. Rec. 1322 (daily ed. Nov. 8, 1989) (testimony of Marc Rotenberg, Director, Computer Professionals for Social Responsibility).

The author is currently a Deputy Maricopa County (Arizona) Attorney; however, the opinions expressed in the article are the author's. the article is not intended to represent the policy of the Maricopa County Attorney's Office. This article is reprinted with the permision of JURIMETRICS JOURNAL. JURIMETRICS JOURNAL is a publication of the American Bar Association Section of Science & Technology and Arizona Stae University of Law Center for the Study of Law, Science & Technology.