Nova Law Review

Volume 21, *Issue* 3 1997 *Article* 5

The Tangled Web We Weave: The Internet and Standing Under the Fourth Amendment

Brian I. Simon*

*

The Tangled Web We Weave: The Internet and Standing Under the Fourth Amendment

TABLE OF CONTENTS

I. INTRODUCTION

"On each landing, opposite the lift shaft, the poster with the enormous face gazed from the wall. It was one of those pictures which are so contrived that the eyes follow you about when you move. BIG BROTHER IS WATCHING YOU, the caption beneath it ran."[1]

1. GEORGE ORWELL, 1984 at 5 (NAL Penguin Inc. 1961).

GEORGE ORWELL was the pen name of an Englishman named Eric Blair. He was born in Bengal in 1903, educated at Eton, and after service with the Indian Imperial Police in Burma, returned to Europe to earn his living writing novels and essays. He was essentially a political writer who wrote of his own times, a man of intense feelings and fierce hates. He hated totalitarianism, and served in the

As we approach the twenty-first century, the Orwellian visions depicted in *1984* seep into our collective consciousness. Has Orwell's nightmare become today's reality? Some would argue that it has.[2]

The increased use of computers, coupled with the advent of cyberspace and the Internet, catapults the criminal defense attorney into a legal arena undreamed of a short time ago. Various sorts of crimes can occur in cyberspace,[3] and as such, criminal procedure issues arising under the Fourth Amendment lurk in the background.

The Fourth Amendment ensures that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable *searches and seizures*, shall not be violated . . . ."[4] If law enforcement officials violate one's Fourth Amendment rights in the process of searching or seizing evidence, the defendant can move to suppress the evidence.[5] However, in order to assert one's Fourth Amendment rights and exclude evidence, the defendant must have *standing*.[6]

> Loyalist forces in the Spanish Civil War. He was critical of communism but considered himself a Socialist. He hated intellectuals, although he was a literary critic. He hated *cant* and lying and cruelty in life and in literature. He died at forty-seven of a neglected lung ailment, leaving behind a substantial body of work, a growing reputation for greatness, and the conviction that modern man was inadequate to cope with the demands of his history.

Preface to GEORGE ORWELL, 1984 (NAL Penguin Inc. 1961) (emphasis added).

2. To connect with others who share the view that we presently exist in an Orwellian world, venture online and see, *EPIC* (visited Apr. 1, 1997) <http://www.epic.org./privacy>.

3. *See* discussion *infra* Part III.A.

4. U.S. CONST. amend. IV (emphasis added).

5. JOSHUA DRESSLER, UNDERSTANDING CRIMINAL PROCEDURE § 109, at 219 (1991). The notion that evidence illegally obtained can be suppressed at trial sprung from the celebrated case of *Boyd v. United States*, 116 U.S. 616 (1886). In *Boyd*, the Court decided that because the government's conduct circumvented the Fourth Amendment when officials forced a citizen to disclose certain incriminating papers, such evidence was inadmissible at trial against the defendant. *Id.* at 631–32 The use of general warrants and writs of assistance, devices employed by agents of the crown in England to rifle through homes of its citizens in an effort to search for evidence, weighed heavily on the minds of the nine justices in *Boyd*. *See generally id.* Accordingly, the development of the exclusionary rule began. *See* discussion *infra* Part II (providing further analysis of the exclusionary rule and its application to the standing doctrine). *See also* Mapp v. Ohio, 367 U.S. 643 (1961); Rochin v. California, 342 U.S. 165 (1952); Wolf v. Colorado, 338 U.S. 25 (1949), *overruled sub nom.* Mapp v. Ohio, 367 U.S. 643 (1961); Weeks v. United States, 232 U.S. 383 (1914), *overruled sub nom.* Mapp v. Ohio, 367 U.S. 643 (1961). The aforementioned cases outline the chronological development of the exclusionary rule.

6. DRESSLER, *supra* note 5, §109, at 219. *See also* discussion *infra* Part II.A.–E.

For purposes of determining whether a defendant may challenge the unconstitutionality of a search and seizure, standing is a threshold question.[7] This note will focus on what constitutes standing for a motion to suppress evidence searched and/or seized in cyberspace. First, the evolution of standing jurisprudence will be discussed. Second, the federal wiretapping statutes will be examined to determine whether they can shed light on this issue. Third, as there are no cases directly on point which focus on standing under the Fourth Amendment and the Internet, two fictional characters, whom you will meet shortly, will take us on various hypothetical journeys through cyberspace and Fourth Amendment analysis.[8]

II. WHAT IS STANDING?

When a defendant challenges the admission of evidence in a criminal case on the premise that it was secured in violation of her Fourth Amendment rights, she must be a party entitled to do so.[9] If the defendant is so entitled, then she has "standing" to move to suppress the evidence *vis-à-vis* the exclusionary rule.[10] The exclusionary rule usually provides that when evidence is unconstitutionally attained, it is inadmissible in criminal proceedings against the person whose rights were violated.[11] This brings us to

7. *See* discussion *infra* Part II.B (explaining *Jones*, *Rakas*, their progeny, and the Court's current stance on standing jurisprudence as a starting point for analysis under the Fourth Amendment).

8. Intriguing criminal cases may flow from the recent Heaven's Gate cult mass suicide. Aside from the cult members' plans to board the mothership they believed to be trailing the Hale-Bopp Comet, a central feature of this peculiar cult was its web site, the "Heavens Gate." (The web site no longer exists.) Will the Heaven's Gate web site prompt legal discussion concerning the Internet and the Fourth Amendment? For interesting discussions concerning the impact of the cult's activity on the Internet, see Robert J. Hawkins & Matt Miller, *Cult Suicide in Rancho Sante Fe: Mass Suicide News Circles the World at Net Speed,* SAN DIEGO UNION & TRIB., Apr. 1, 1997, at 12 (Computer Link Section); Sandi Dolbee, *Cult Suicide in Rancho Sante Fe: 18-year-old Recounts His Internet Visit with Cultist Sandi Dolbee,* SAN DIEGO UNION & TRIB., Mar. 30, 1997, at A1; and James Lileks, *Cult Suicide in Rancho Sante Fe: Death Cult Fantasy Disguised as Religion Drove Heaven's Gate Cultists to Delusion, and Ultimately to Self-Destruction; 'New Age' Indulgence Led Odd People to Bizarre End,* SAN DIEGO UNION & TRIB., Apr. 1, 1997, at G1.

9. WAYNE R. LAFAVE & JEROLD ISRAEL, CRIMINAL PROCEDURE § 9.1, at 459–60 (1992).

10. DRESSLER, *supra* note 5, at 219.

11. *Id.* at 235. However, if police officers, in good faith, reasonably rely on what is later determined to be an invalid warrant, the evidence may be used against the defendant at his or her trial. *See* United States v. Leon, 468 U.S. 897 (1984). *Leon* firmly established the "good faith" exception to the exclusionary rule. *See* DRESSLER, *supra* note 5, at 249–50. *See also* United States v. Haven, 446 U.S. 620 (1980); Harris v. New York, 401 U.S. 222 (1971);

the central issue: When does the defendant have standing; in other words, when is one entitled to challenge the admission of evidence on grounds that the search and seizure contravened the Fourth Amendment?

A. Katz v. United States

The linchpin for standing, and Fourth Amendment examination in general, hinges on *Katz v. United States*.[12] When Charles Katz called in his wagers from a public telephone booth in Los Angeles, BIG BROTHER was listening. Without a warrant, FBI agents surreptitiously attached electronic listening and recording devices to the *outside* portion of the booth where Mr. Katz placed his calls.[13]

Prior to the *Katz* decision, Fourth Amendment jurisprudence encompassed the rationale that physical penetration or trespass into a "constitutionally protected area" was necessary for governmental conduct to rise to the level of a violation under the Fourth Amendment.[14] The logical implication of this standard translated into a legal principle which espoused a property based model for determining whether a defendant had standing.[15] Thus, before *Katz*, standing was invariably entwined with the Court's property based approach to Fourth Amendment jurisprudence.[16]

It therefore came as no surprise that the government in *Katz* argued no search occurred because there was no physical trespass into the phone booth

---

Walder v. United States, 347 U.S. 62 (1954); Agnello v. United States, 269 U.S. 20 (1925). These cases discuss the chronological development of the exception to the exclusionary rule for purposes of impeaching a defendant's credibility. *See also* Nix v. Williams, 467 U.S. 431 (1984) (explaining the inevitable discovery exception to the exclusionary rule which states that evidence which would otherwise be inadmissible because of an unconstitutional search or seizure transforms into admissible evidence if in the final analysis, the evidence would have been lawfully discovered independent of the initial bad search or seizure).

12. 389 U.S. 347 (1967).

13. *Id.* at 348–49. The physical location of the listening device, the outside portion of the phone booth, is meaningful in that the Court's Fourth Amendment philosophy, up to this point in history, hinged on whether there was physical penetration into a "constitutionally protected area." If the Court adhered to its prior rationale, there could not be a Fourth Amendment violation in *Katz* because the listening device did not actually penetrate any of the four walls of the phone booth.

14. Olmstead v. United States, 277 U.S. 438 (1928). In *Olmstead*, government agents intercepted the defendant's phone conversations without any physical trespass into the defendant's home. The Court deduced that without a physical trespass, no search of a place could have occurred under the rubric of the Fourth Amendment. *Id.* at 466.

15. WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 11.3, at 118 (1996).

16. DRESSLER, *supra* note 5, at 56.

where Mr. Katz called in his bets.[17] Katz was convicted, and the district court, as well as the court of appeals, agreed on admitting the tape recorded evidence.[18] Both lower courts relied on the logic of *Olmstead v. United States* and its progeny, ruling that no violation occurred because there was no physical invasion of the phone booth where Mr. Katz placed his calls.[19]

Justice Stewart, writing for the majority, rejected the trespass rationale stemming from *Olmstead*, stating the now oft-quoted phrase that "the Fourth Amendment protects people, not places."[20] His opinion, read together with Justice Harlan's concurring opinion, formed the crux for future Fourth Amendment jurisprudence.[21] Standing would no longer be contingent upon whether there was a physical intrusion into the area being searched. Justice Harlan's concurrence advocated a two prong test: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[22] While the subjective prong is no longer critical to the overall calculus for determining whether one has standing, both prongs still must be satisfied.[23] In fact, some contend that "inquiry into the particular defendant's subjective state of mind has *no* place in the application of the *Katz* expectation of privacy standard."[24] The focus of the objective prong examines what types of self-protective steps were taken by the individual to ensure that his or her activities would remain private.[25] Were those self-protective steps *sufficient* to justify a reasonable person in believing that his or her activity would be free from uninvited eyes or ears? One who knowingly exposes her activities to the public or acts in plain view, cannot be said to have a reasonable expectation of privacy.[26] In the same vein, the Fourth Amendment does not protect a wrongdoer's misplaced belief that a person to whom he voluntarily confides information will not reveal it to the government.[27]

---

17. *Katz*, 389 U.S. at 352.

18. Katz v. United States, 369 F.2d 130, 134 (9th Cir.), 389 U.S. 347 (1967).

19. *Id.* at 133.

20. *Katz*, 389 U.S. at 351. Individual privacy (it was thought), not the arbitrary location of a listening device, would be the detrimental factor for Fourth Amendment jurisprudence. *See also* LAFAVE & ISRAEL, *supra* note 9, at 248.

21. DRESSLER, *supra* note 5, at 58–59.

22. *Katz*, 398 U.S. at 361 (Harlan, J., concurring).

23. DRESSLER, *supra* note 5, at 60.

24. LAFAVE, *supra* note 15, § 11.3(c), at 157.

25. DRESSLER, *supra* note 5, at 63.

26. *Katz*, 389 U.S. at 351.

27. Hoffa v. United States, 385 U.S. 293, 302 (1967). Although *Hoffa* was not grounded precisely on the standing issue, its logic is certainly relevant to the overall calculus as to whether one has a reasonable expectation of privacy. This is because "the Fourth Amendment

Applying this test to the facts in *Katz*, we can easily see why the FBI surveillance constituted a search. First, Katz must have had an actual expectation of privacy when he placed the call in the phone booth. Katz did not know the phone booth was being monitored by the FBI; therefore, when he picked up the phone, he had an actual expectation of privacy. Second, Katz stepped into the phone booth and shut the door behind him before placing his calls. He took adequate self-protective steps. Justice Stewart points out that he did this to exclude the "uninvited ear."[28] "One who occupies it [the phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[29]

Despite abandoning the trespass rationale grounded in *Olmstead*, the Court will sometimes utilize property concepts for purposes of standing analysis.[30] However, the Court is often weary of a property-based approach to standing and prefers to tailor its reasoning to the *Katz* expectation of privacy test.[31] Nevertheless, the property-based rationale can be reconciled with the approach *Katz* takes.[32]

> The fundamental inquiry regarding standing to object to a search is that articulated in [*Katz* and] *Mancusi:* whether the conduct which the defendant wants to put in issue involved an intrusion into *his* reasonable expectation of privacy. In resolving that question, it is useful to consider the factors which the Court has on other occasions alluded to—whether the defendant had an interest in the place searched, whether he had an interest in the items seized, and

---

[does not] protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. This simple but crucial line of reasoning will play an important role in the system operator/user relationship on the Internet for purposes of determining whether the user has standing to object to evidence obtained in cyberspace. *See* discussion *infra* Parts IV.A.–F.

28. *Katz*, 389 U.S. at 352.

29. *Id.*

30. LAFAVE, *supra* note 15, § 11.3, at 118. "[S]tanding may be acquired by having a 'proprietary or possessory interest in the premises' which were searched . . . ." *Id.* (quoting Brown v. United States, 411 U.S. 223, 229 (1973)).

31. *See* Mancusi v. DeForte, 392 U.S. 364 (1968). The Court held that the "capacity to claim the protection of the [Fourth] Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion." *Id.* at 368.

32. LAFAVE, *supra* note 15, § 11.3, at 119.

> whether the search occurred at a place where he was lawfully present.[33]

Thus, while physical trespass is not dispositive on the issue of standing, the utilization of property concepts will aid in the determination of whether a particular defendant has standing.

B. Jones, Rakas, *and Their Progeny*

Rakas v. Illinois[34] is considered the leading modern Supreme Court case for standing under the Fourth Amendment.[35] In *Rakas*, police officers pulled over an automobile which matched the description of a vehicle used in a robbery.[36] They searched the car and found evidence of the robbery, including a sawed-off shotgun underneath the front passenger seat and rifle shells in a locked glove compartment.[37] The defendant, a passenger, moved to exclude the evidence on grounds that the search violated his Fourth Amendment rights.[38] Relying on the Court's 1960 decision in *Jones v. United States*,[39] the defendant contended he had standing to contest the search because he was "'legitimately on [the] premises'" when the police examined the car.[40]

In *Jones*, the defendant, a guest at another's apartment, was present when police searched the apartment and found contraband.[41] The defendant testified that the apartment belonged to a friend who had given him a key and permission to use the apartment.[42] Under its interpretation of Rule 41(e) of the *Federal Rules of Criminal Procedure*,[43] the Court announced that

---

33. *Id.* (footnote omitted).
34. 439 U.S. 128 (1978).
35. DRESSLER, *supra* note 5, at 224.
36. 439 U.S. at 130.
37. *Id.*
38. *Id.*
39. 362 U.S. 257 (1960), *overruled sub nom.* United States v. Salvucci, 448 U.S. 83 (1980).
40. *Rakas*, 439 U.S. at 132 (alteration in original).
41. 362 U.S. at 259.
42. *Id.*
43. Rule 41 states:

> (e) Motion for Return of Property. *A person aggrieved by an unlawful search and seizure* or by the deprivation of property may move the district court for the district in which the property was seized for the return of the property on the ground that such person is entitled to lawful possession of the property. The court shall receive evidence on any issue of fact necessary to the decision of the motion. If the motion is granted, the property shall be returned to the movant, although reasonable conditions may be imposed to protect access and the use of

"anyone legitimately on premises" at the time of the search qualified "as a 'person aggrieved by an unlawful search and seizure'"[44] and had standing to move to suppress the evidence.[45] Lower courts utilized this "legitimately on premises" rationale as a basis for determining whether a defendant had standing under the Fourth Amendment.[46]

The Court dismissed that line of logic in *Rakas*,[47] and instead couched its language for standing in terms of the doctrine espoused in *Katz*: Does the individual have a "legitimate expectation of privacy in the invaded place?"[48] Justice Rehnquist, speaking for a 5-4 majority, conservatively construed the following rationale found in *Alderman v. United States*:[49] "'Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.'"[50]

Despite retreating from the "legitimately on premises" rationale grounded in *Jones*, the Court upheld the lower court's holding through the

---

> the property in subsequent proceedings. If a motion for return of property is made or comes on for hearing in the district of trial after an indictment or information is filed, it shall be treated also as a motion to suppress under Rule 12.

FED. R. CRIM. P. 41(e) (emphasis added).

44. *Jones*, 362 U.S. at 261 (quoting FED. R. CRIM. P. 41(e)).

45. *Id.* at 267.

46. *See* State v. Porter, 324 N.E.2d 857 (Ind. Ct. App. 1975); Commonwealth v. Tasco, 323 A.2d 831 (Pa. Super. Ct. 1974); State v. Simms, 516 P.2d 1088 (Wash. Ct. App. 1973). These cases all hold that guests who were legitimately on premises have standing to challenge the admission of evidence to be used against them.

47. This will prove to be important because an Internet user who is at a website with the system operator's permission (legitimately on premises) may not automatically attain standing to challenge evidence searched and seized in cyberspace. *See* discussion *infra* Part IV.

48. *Rakas*, 439 U.S. at 143.

49. 394 U.S. 165 (1969). In *Alderman*, the Court crystallized the contention that Fourth Amendment rights are personal:

> There is no necessity to exclude evidence against one defendant in order to protect the rights of another. . . . What petitioners appear to assert is an independent constitutional right of their own to exclude relevant and probative evidence because it was seized from another in violation of the Fourth Amendment. But we think there is a substantial difference for constitutional purposes between preventing the incrimination of a defendant through the very evidence illegally seized from him and suppressing evidence on the motion of a party who cannot claim this predicate for exclusion.

Id. at 174. This argument is vital to understanding the predicament of the online user and her relationship with the system operator. A user may not be able to assert a Fourth Amendment violation if only the system operator's rights are violated. *See* discussion *infra* parts IV.A.-F.

50. *Rakas*, 439 U.S. at 133–34 (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)).

use of the *Katz* framework[51] and some crafty *post hoc* analysis. Thus, the Court did not directly overrule the "legitimately on premises" rationale in all cases. Rather, this factor should be considered in conjunction with a determination as to whether the particular defendant's situation parallels the circumstances in *Jones*. The Court reasoned that Rakas, though legitimately on the premises (in the car), did not have a reasonable expectation of privacy similar to Jones. Unlike Rakas, Jones had a key to the apartment, clothes in the closet, and had previously slept on the premises.[52] Those facts indicate complete dominion and control and the power to exclude others from the apartment.[53] "[D]ominion and control" and the power to exclude others are integral components of the objective prong to the *Katz* test.[54] The key Jones possessed, in addition to the clothes he stored in the apartment, were sufficient indicia of control to warrant an expectation of privacy that "society is prepared to recognize as 'reasonable.'"[55] The Court also elucidated that because the right to exclude others invariably flows from the ownership or lawful possession of real or personal property, one who has such a possessory interest will probably have a legitimate expectation of privacy stemming from that right to exclude.[56]

Unlike Katz and Jones, Rakas did not have any indicia of control.[57] Katz occupied the telephone booth, shut the door behind him to exclude all others, and paid the toll.[58] "Except with respect to his friend, Jones had complete dominion and control over the apartment and could exclude others from it."[59] Here, Rakas simply could not prove he had a legitimate expectation of privacy as a mere passenger in an automobile contesting the search of

---

51. *Id.* at 141. Why did the Court retreat from the "legitimately on premises" rationale found in *Jones?*

> [T]he holding in *Jones* can best be explained by the fact that Jones had a legitimate expectation of privacy in the premises he was using and therefore could claim the protection of the Fourth Amendment with respect to a governmental invasion of those premises, even though his "interest" in those premises might not have been a recognized property interest at common law.

Id. at 143.

52. *Id.* at 141.

53. *Id.* at 143–44 n.12.

54. *Rakas*, 439 U.S. at 149.

55. *Katz*, 389 U.S. at 361.

56. *Rakas*, 439 U.S. at 143–44 n.12.

57. Essentially, Rakas could not *legitimately* exclude others from the automobile because he did not have a possessory interest in it. *See* discussion *supra* notes 54–56 and accompanying text.

58. *Rakas*, 439 U.S. at 149.

59. *Id.*

contraband found under the seat and in a glove compartment.[60] Therefore, Rakas did not have standing to assert the illegality of the search in an attempt to suppress the evidence seized.[61]

Interwoven within standing analysis under the Fourth Amendment is the issue of whether a search has occurred. Because the Fourth Amendment only protects against unreasonable searches and seizures, it could not come into play with out a search. To determine whether government activity rises to the level of a search within the meaning of the Fourth Amendment, one must have a legitimate expectation of privacy in the area examined.[62] Essentially, this is the same test used to determine whether a defendant has standing to challenge the admission of evidence. The basic similarity between the tests for standing and determining whether a search occurred led Justice Rehnquist to opine in *Rakas*: "The inquiry under either approach is the same. But we think the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing."[63]

Despite Justice Rehnquist's position, two years later, in *Rawlings v. Kentucky*,[64] Justice Blackmun contended:

> [T]hat these two inquiries [standing and whether a substantive Fourth Amendment 'search' occurred] 'merge into one' in the sense that both are to be addressed under the principles of Fourth Amendment analysis developed in Katz v. United States and its progeny. But I do not read . . . *Rakas*[] as holding that it is improper for lower courts to treat these inquiries as distinct components of a Fourth Amendment claim.[65]

---

60. *Id.* Arguably if Rakas has a key to the car, he would have had standing.

61. *Id.*

62. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

63. *Rakas*, 439 U.S. at 139 (footnote omitted).

64. 448 U.S. 98 (1980).

65. *Id.* at 112 (Blackmun J., concurring) (citations omitted). In *Rawlings*, the defendant was the unsuspecting guest at the house of one Marcuess who had the misfortune of being present when the police searched the Marcuess home without a warrant. Apparently, seconds before the police arrived, the defendant stuffed some 1,800 tablets of LSD and other drugs into another guest's (Vannessa Cox) purse. Although the defendant had a possessory interest in the contraband seized, the Court concluded that he did not have a legitimate expectation of privacy in Cox's purse. *Id.* at 105–06. Defendant could not exclude others from Cox's purse and had no dominion and control over it. *Id.* Thus, the defendant did not have standing. *Id.* One can foresee the applicability of *Rawlings* on the Internet. The fact that one might have a

Justice Blackmun pointed out that it is possible for a defendant to have standing but lose on the merits.[66] Conversely, one could win on the merits yet have no legitimate expectation of privacy for purposes of standing.[67] In the final analysis, however, if the defendant loses either the standing issue or on the merits, the evidence will be admissible. To successfully win a motion to suppress evidence, one must have standing *and* there must be a "search" under substantive Fourth Amendment analysis.[68]

C. *Hotels, Motels, Tenants, and the Transfer of Property*

Does an individual have a reasonable expectation of privacy in a leasehold, hotel, or motel room when he or she is not there at the time of the government search?[69] At first blush, some might contend that because the hotel or motel manager has a possessory interest in the establishment, as well as the potential to access its rooms, one cannot have a reasonable expectation of privacy. Such an argument necessarily encompasses a rationale that the landlord or manager can validly consent to a government agent's request to search the tenant's or guest's premises. This sort of argument has been consistently rejected by courts facing the issue.

Courts have determined that those tenants,[70] hotel guests,[71] and motel guests[72] with a present possessory interest in the premises searched all have

---

possessory interest in one's electronic mail does not necessarily mean one will have standing. If one lacks dominion and control or the power to exclude others from their electronic mail, the possessory interest in it becomes irrelevant.

66. *Rawlings*, 448 U.S. at 105–06.

67. *Id.*

68. It is useful to examine cases stemming from both of these issues to assess their applicability to the Internet. *See also* United States v. Salvucci, 448 U.S. 83 (1980) (rejecting the automatic standing doctrine for possession offenses and developing the chronological analysis under the standing doctrine). *Salvucci* sheds light on *Rakas*. Interview with Professor Mark Dobson, Nova Southeastern University, Shepard Broad Law Center (Feb. 18, 1997).

69. Standing in these types of situations is important because some will contend that the relationship between a user and her system operator is the functional equivalent of the hotel guest and manager relationship. If these types of relationships are indeed analogs of each other, then the case for standing in cyberspace dramatically improves because hotel and motel guests typically have standing to assert the illegality of a search. *See infra* Part IV (providing additional discussion on this argument).

70. *See, e.g.*, Chapman v. United States, 365 U.S. 610 (1961); United States v. Ford, 34 F.3d 992 (11th Cir. 1994). These cases stand for the proposition that one with a leasehold interest (as opposed to ownership) has standing to challenge a government search. Under a *Katz-Mancusi* analysis, a defendant would have a legitimate expectation of privacy for purposes of standing. *See* LAFAVE, *supra* note 15, § 11.3(a), at 122.

71. *See, e.g.*, Stoner v. California, 376 U.S. 483 (1964); State v. Jackson, 210 N.W.2d 537 (Iowa 1973). Both cases hold that the consent of a hotel clerk obtained by police to search defendant's room was invalid. Under a *Katz-Mancusi* analysis, the defendant would

standing to challenge evidence obtained by the government.[73] Thus, managers and landlords may not always effectively consent to the search of their tenants rooms. For example, tenants and paying guests could *effectively* consent with their landlords or managers to allow the police to search their rooms. Such consent would obliterate the legitimate expectation of privacy necessary for standing.

D. *Self-Protective Steps and Modern Technology*

What constitutes a self-protective step that would rise to the level of a reasonable expectation of privacy? Technology has advanced to a point where activities once considered private are, for purposes of standing jurisprudence under the Fourth Amendment, "broadcast to the world."[74]

In *Smith v. Maryland*,[75] the Court ruled that the defendant had no legitimate expectation of privacy in the phone numbers he dialed from his home.[76] Police used a device called a pen register to monitor the electrical impulses coming from the defendant's phone in order to compile a list of the numbers he called.[77] The Court applied *Katz* and determined that the defendant probably could not have an actual expectation of privacy in the phone numbers he dialed because he knowingly divulged that information to the telephone company.[78] Second, assuming arguendo one did have an actual expectation of privacy in the phone number she dialed, such an expectation could not be reasonable.[79] Following the line of logic in *Hoffa* and it's progeny, one who voluntarily conveys information to a third party cannot have a reasonable expectation of privacy.[80] *Katz* was distinguished on the ground that pen registers do not disclose the contents of one's conversations, only the numbers dialed.[81] Where one has a reasonable expectation of privacy in the contents of her conversation, she does not with

---

have a legitimate expectation of privacy for purposes of standing. *See* LAFAVE, *supra* note 15, § 11.3(a), at 122.

72. *See, e.g.*, United States v. Anderson, 453 F.2d 174, 177–78 n.6 (9th Cir. 1971) (relying on *Jones* in order to deduce that a motel guest has standing). Utilizing the *Katz-Mancusi* analysis, a defendant in a motel room would have a legitimate expectation of privacy in such premises for purposes of standing. *See* LAFAVE, *supra* note 15, § 11.3(a), at 122.

73. *See generally* LAFAVE, *supra* note 15, § 11.3(a).

74. *Katz*, 389 U.S. at 352.

75. 442 U.S. 735 (1979).

76. *Id.* at 742.

77. *Id.* at 736 n.1.

78. *Id.* at 742.

79. *Id.* at 743.

80. *Smith*, 442 U.S. at 743–44.

81. *Id.* at 741.

the numbers she dialed.[82] The phone company must track the phone numbers dialed for purposes of billing.[83] A phone company does not have a similar need for the contents of the user's communications.[84] Therefore, a defendant like Smith will not have standing to assert the illegality of a search for phone numbers dialed.

The use of beepers to track a suspect's movements is not considered a search under constitutional analysis if the information it communicates is available to the general public, or if such information could be gathered from an area where one is legally entitled to watch.[85] If information is secured through the use of a beeper from an area not within the public's view, then such activity is considered a search under the Fourth Amendment.[86]

In *Dow Chemical Co. v. United States*,[87] the Court held that no search occurred when the government engaged in aerial photography to secure pictures of an industrial complex.[88] Although Dow Chemical Company constructed walls around their complex preventing ground-level view,[89] such self-protective steps were not legally sufficient.[90] Because the plane's surveillance occurred from public navigable airspace and was not physically intrusive, the self-protective steps taken by Dow were rendered meaningless because they did not cloak what could be seen from above.[91] The Court noted in dictum that the use of "highly sophisticated surveillance not generally available to the public, such as satellite technology,"[92] might constitute a search under the Fourth Amendment.

The dissent pointed out the fallacious logic in the majority opinion: How could the $22,000, precision aerial mapping camera the government used be considered readily available to the public?[93] Who would purchase such a device? From *Dow Chemical*, it would seem that if sense-enhancing technology is available (like a precision aerial mapping camera), then the use of it can not be considered a search. However, the use of sense-creation devices (like satellite technology) probably would constitute a search under

82. *Id.*
83. *Id.* at 744.
84. *Id.*
85. United States v. Knotts, 460 U.S. 276 (1983).
86. *Id.*
87. 476 U.S. 227 (1986).
88. *Id.* at 239.
89. *Id.* at 229.
90. *Id.* at 239.
91. *Id.* at 238–39.
92. *Dow Chemical*, 476 U.S. at 238.
93. *Id.* at 251 n.13 (Powell, J., dissenting).

the Fourth Amendment. What one knowingly exposes to the public must be done at one's peril. If BIG BROTHER can potentially watch from a public view, he can legally watch.

One other case of note, *California v. Greenwood*,[94] holds that one cannot have a reasonable expectation of privacy in the contents of her garbage left at the side of the curb.[95] The Court cited to both *Katz* and *Smith*, reasoning that garbage is knowingly exposed to the public and voluntarily turned over to a third party (the garbage collector).[96] The crux of *Greenwood* in reality went further than *Katz* and *Smith*. Greenwood only knowingly exposed opaque garbage bags to the public, *not* the contents inside the bag. The majority worked around this obstacle by reasoning that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[97] Thus, one cannot have a reasonable expectation of privacy in the garbage he discards at curbside. The Court "emphasized instead that the Fourth Amendment analysis must turn on such factors as 'our *societal* understanding that certain areas deserve the most scrupulous protection from government invasion.'"[98]

The Court also reasoned that a California law declaring the search of trash illegal, and providing for use of the exclusionary rule as a means of remedying such illegality, does not allow an individual's expectation of privacy to rise to the level of a "reasonable" one under the Fourth Amendment.[99] State law does not define whether one has a reasonable expectation of privacy.[100] Similarly, in a case where police broke the law and trespassed on the defendant's property to search for marijuana, despite "no trespassing" signs, the Court held that one could not have a legitimate expectation of privacy because the area invaded was an open field.[101]

94. 486 U.S. 35 (1988).

95. *Id.* at 41.

96. *Id.* at 40.

97. *Id.* (footnotes omitted) (citation omitted). The garbage ultimately goes to the dump where people, along with thousands of vultures, can view and peck at the contents of everyone's rubbish. Say au revoir to any reasonable expectation of privacy!

98. *Id.* at 43. (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)). The Court now seems to be injecting society's common knowledge and understanding into the calculus of what constitutes a legitimate expectation of privacy.

99. *Greenwood*, 486 U.S. at 43.

100. *Id.*

101. Oliver v. United States, 466 U.S. 170 (1984).

E. *Flaws in the Federal Wiretapping Statutes*

In 1986, Congress revamped federal wiretapping statutes to include the prohibition on the interception of electronic communications.[102] Commonly known as the Electronic Communications Privacy Act ("ECPA"),[103] this statute purports to govern the procedures for obtaining information online. As with many statutes, the ECPA is riddled with exceptions.[104]

Section 2510(12) defines an "electronic communication" as "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."[105] Although the ECPA prohibits the interception and disclosure of wire, oral, or electronic communications,[106] it permits any person "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[107] This language encompasses the rationale in *Katz* and authorizes the interception of those electronic communications knowingly exposed to the public.

The ECPA also carves out an exception permitting one to disclose the contents of electronic communications "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a

---

102. LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD 167 (1995) [hereinafter NETLAW].

103. 18 U.S.C. § 2510 (1994).

104. It should also be noted that there are no cases which apply the ECPA to a situation involving the interception of communications in cyberspace.

105. 18 U.S.C. § 2510(12). Not included in the definition of an electronic communication is a wire or oral communication. *See id.* § 2510(12)(A).

> "[W]ire communication" means 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 . . . communications . . . .

Id. § 2510(1). "'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *Id.* § 2510(2). These definitions will prove to be important because the ECPA only authorizes the suppression of evidence when oral and wire communications are intercepted.

106. *Id.* § 2511 (1994).

107. 18 U.S.C. § 2511(2)(g)(i).

crime, if such divulgence is made to a law enforcement agency."[108] Thus, if the service provider "inadvertently" stumbles across some evidence tending to incriminate her user, she may divulge the contents of the user's communications to the police. The crux of the ECPA, as it pertains to the prohibition on divulging the contents of an electronic communication, is found in section 2511(3)(a) which states that

> a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) *while in transmission* on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.[109]

The words "while in transmission" are crucial to understanding the ECPA. Because the ECPA only protects against the divulging of communications "while in transmission," it is logical to deduce that stored messages are beyond the reach of the statute.

> [T]he ECPA does not give online system users an automatic right of privacy from system operators for stored messages. Since a system can easily be configured to store all messages that pass through it, the ability to review stored messages effectively gives the operator the ability to review all messages passing through the system.[110]

Of course, a provider of an electronic communication service may divulge the contents of electronic communications if he or she has been provided with "a court order directing such assistance signed by the authorizing judge."[111] A properly executed warrant authorizes the service provider to assist law enforcement officials in intercepting electronic communications.

Assuming arguendo the electronic communication is "in transmission" within the meaning of section 2511(3)(a), it remains unclear whether one will be able to remedy the interception of such communications through a

---

108. *Id.* § 2511(3)(b)(iv).

109. *Id.* § 2511(3)(a) (emphasis added).

110. NETLAW, *supra* note 102, at 168. The ECPA would prohibit the interception and disclosure of electronic messages sent in live or real-time transmission. *Id.*

111. 18 U.S.C. § 2511(2)(a)(ii)(A).

motion to suppress evidence. Section 2515[112] only prohibits the use of evidence of intercepted wire or oral communications.[113] This section does not mention an "electronic communication" as a type of communication which would require the prohibition of its use as evidence.[114] The canon *expressio unius est exclusio alterious* leads one to conclude that because the drafters of the ECPA specifically mentioned the words "wire" and "oral communications" in section 2515, the words "electronic communications" must have been intentionally omitted since such words would have been included if that was what the legislature had intended.[115] The ECPA seemingly affords the greatest amount of privacy protection for aural transmissions[116] (a type of transmission not encompassed in the definition of "electronic communications"). The only remedy mentioned for an unauthorized interception or disclosure of an electronic communication is a civil cause of action under section 2520.[117]

It would seem as though the ECPA, like many laws, has loopholes which would curtail a user's privacy for purposes of standing under the Fourth Amendment. The issue of whether a particular defendant has standing to initiate a motion to suppress evidence will most likely have to be

---

112. 18 U.S.C. § 2515 (1994).

113. Section 2515, entitled "Prohibition of use as evidence intercepted wire or oral communications," states:

> 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.

Id. (emphasis added).

114. *See id.*

115. The following canon should play a significant role in the interpretation of § 2515: "Technical and legal words with special meanings are construed according to the technical, legal, or special meaning appropriate to the context of the statute." JACK DAVIES, LEGISLATIVE LAW AND PROCESS IN A NUTSHELL 311 (1986). This canon futher buttresses the argument that the drafters intended "electronic communications" to be omitted from the scope of § 2515. Accordingly, the meanings of the words electronic, oral, and wire communications, which are "technical and legal words," should be treated the same throughout the ECPA. The words are "technical" in the sense that they deal with highly particularized modes of communication. They are "legal" because they must be construed within the meaning of a law, the ECPA. Simply put, the ECPA does not explicitly, or even implicitly, authorize the suppression of an electronic communication.

116. NETLAW, *supra* note 102, at 168.

117. *See generally* 18 U.S.C. § 2520 (1994).

resolved by resorting to the seminal Fourth Amendment cases discussed above.[118]

III. CYBERSPACE

> Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multi-dimensional, artificial, or "virtual" reality. In this world, on which every computer screen is a window, actual, geographic distance is irrelevant. Objects seen or heard are neither physical nor, necessarily, presentations of physical objects, but are rather—in form, character, and action—made up of data, pure information. This information is derived in part from the operation of the natural, physical world, but is derived primarily from the immense traffic of symbolic information, images, sounds, and people, that constitute human enterprise in science, art, business, and culture.[119]

Because there are so many different methods of accessing cyberspace, various legal theories will apply to different factual scenarios. This note will focus only on the potential legal pitfalls in the "public system" which provides access to the general public as a whole. Such a system typically includes a storage area in cyberspace where one can access his or her own data and prevent others from retrieving it (through the use of a password). Additionally, there are areas where all have access to the same information.

A system operator (also referred to as a "sysop") is one who heads the particular online system. System operators who run these systems have the ability to access one's "private" files but may or may not choose to do so.[120] Within the web of "public" cyberspace, there might also be some systems existing which provide users limited access. In order to gain access to such a system, a user might have to pay a fee or obtain approval from the system operator who runs it.

A. *Online Crime and Evidence of Crime Online*

New societal conventions seem to go hand in hand with new forms of crime. Even those who have never gone online know about the problems

118. *See also* Megan Connor Bertron, Note, *Home Is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163 (1996).

119. M. ETHAN KATSH, LAW IN A DIGITAL WORLD 29 (1995).

120. *See generally* NETLAW, *supra* note 102; *see also supra* notes 108–17 and accompanying text.

with hackers in cyberspace.[121] The word "hacker" was not in existence until computers linked up with telecommunications.

Aside from hacking, various forms of computer crime now exist. Criminals upload viruses in an attempt to destroy computer systems, steal copyrighted material, and engage in the exchange of child pornography amongst other things.[122] Private files exist which contain evidence of crime occurring outside cyberspace (the dreaded physical world).[123] If police "search" cyberspace, the question of standing to assert the illegality of government conduct becomes pertinent.

B. *Meet Stoney and Talley*[124]

In order to better understand how standing under the Fourth Amendment works in conjunction with cyberspace, we will follow the exploits of two fictional characters named Stoney and Talley. Stoney and Talley are your stereotypical cyber-nerds who have a knack of getting into trouble while surfing the net.

IV. SIX HYPOTHETICALS

A. *The "Public" Chat Room*

The Dean of Admissions at the newly-established Cyber Law Center would ultimately regret rejecting Stoney and Talley to the class of 2000. Upon receiving their e-mail rejections from the Cyber Law Center, Stoney and Talley decided to discuss their options at the "Worms R' Us" site on the web where all the expert hackers did their business.

Both entered the site from their computers at home and joined Public Chat Room No. 3—a forum for disgruntled law school rejects. No password or fee was required to join Public Chat Room No. 3. "All are Welcome" blinked across the screen as they logged in. The top of the screen indicated 29 users who were currently in the room. Stoney and Talley bragged to all who would listen about their detailed plot to upload a destructive worm into the Cyber Law Center.

---

121. *Id.* at 141.
122. *Id.* at 187–208.
123. *Id.*
124. Professor Johnny C. Burris of Nova Southeastern University, Shepard Broad Law Center created these names for a hypothetical problem he distributed to his Criminal Procedure class in the Summer of 1995.

What Stoney and Talley couldn't know was that Officer Iago McFadden, a veteran of the Cleveland Police force, was masquerading online as Earthworm Jim, a supposed world-famous hacker. Warrantless online eavesdropping had become second nature to McFadden after the Cleveland brass moved him behind a desk and off the streets of Ohio. McFadden downloaded the incriminating conversations to his computer and later arrested Stoney and Talley for attempted computer tampering. At a pre-trial conference, Stoney and Talley moved to suppress the evidence on grounds that McFadden's search violated their Fourth Amendment rights.

Would Stoney and Talley have standing to assert the illegality of Officer McFadden's search? Clearly they would not. Under *Katz*, neither could have an actual (subjective) expectation of privacy in the contents of their communications because Public Chat Room No. 3 was open to the public. They both had to know that anyone online could see what they were saying. Assuming arguendo they did have an actual expectation of privacy, they could not have standing under the objective prong of the *Katz* analysis. Stoney and Talley knowingly exposed their conversation to the public. They took no self-protective steps to ensure privacy, and had no indicia of control to exclude others from the room. Furthermore, *Hoffa* tells us that the Fourth Amendment does not protect a wrongdoer's misplaced belief that a person to whom he voluntarily confides information will not reveal it to the government.[125] Thus, it would appear that any expectation of privacy they might have had would not be one which society would recognize as reasonable. The ECPA is in accordance with such analysis as it provides for the lawful interception of those electronic communications which are readily available to the public.[126] Inherent within the concept of a public chat room is the principle that everyone can see what everyone else is saying. It is therefore impossible to have a legitimate expectation of privacy in public chat rooms.

B. *The "Private" Chat Room*

Same scenario as before, except this time: *Stoney and Talley decide to discuss their plot to destroy the Cyber Law Center in "The Worm Hole" a "private"[127] chat room and sub-cite of "Worms R' Us." Other users are excluded from this area and may only view communications posted in the public chat room. Only the "Worms R' Us" system operator can view messages being transferred in private chat rooms like "The Worm Hole."*

125. *Hoffa*, 385 U.S. at 302.

126. *See* 18 U.S.C. § 2511(2)(g)(i).

127. It was "private" in the sense that the word "private" blinked across the top of their screens.

Sysop Slug, the system operator for "Worms R' Us," configured her system to store all messages passed online in both the public and private chat rooms. It is common knowledge that system operators can view messages stored in the computer and are capable of viewing live chat room discussions as well.

Hot on the trail of Stoney and Talley and tired of his desk job, Eagle-Eye McFadden takes to the streets and proceeds to (without a warrant) shakedown Sysop Slug for any information she might have on the two notorious hackers he'd been following. Reluctantly, Sysop Slug turns over the information. Stoney and Talley are arrested and they move to suppress the evidence McFadden gathered.

A few wrinkles develop in the previous hypothetical. First, when Stoney and Talley entered into "The Worm Hole," their case for an actual (subjective) expectation of privacy becomes more plausible if they really thought it was a "private" chat room. If both offer solid proof that they thought their communications would not be read by anyone, including Sysop Slug or eavesdropping hackers and users, it would be tough to overcome their assertion of a subjective expectation of privacy. Standing in this instance will (as it almost invariably does) turn on whether Stoney and Talley had a *legitimate* expectation of privacy. Stoney and Talley will contend that stepping into the "private" room constituted a self-protective step sufficient to rise to the level of a reasonable expectation of privacy. By doing so, they had dominion and control of their online conversation and had the power to exclude others from viewing it.

A cursory inspection of the former argument might seem persuasive. In fact, the *Katz* Court might have found a reasonable expectation of privacy. Under the logic of *Greenwood* and *Oliver*, however, it is generally understood by society that system operators have access to monitor all areas within their control and are truly considered the biggest threat to online privacy.[128] System operators fear potential raids by government agents chasing cyber-criminals.[129] This fear prompts many system operators to "reduce or eliminate user privacy on the system."[130]

Assuming arguendo this sort of societal understanding is empirically true, one cannot have a legitimate expectation of privacy in a "private" chat room under the logic of *Greenwood* and *Oliver*. If the possibility of snoops rummaging through our garbage does not create a legitimate expectation of privacy based on our common knowledge, it requires a simple extension of

128. NETLAW, *supra* note 102, at 166.
129. *Id.*
130. *Id.*

the *Greenwood* holding to argue that a sysop's control of users' data renders an expectation of privacy illegitimate even in a "private" chat room when society recognizes the existence of this type of sysop control.

Under the logic of the ECPA, because Sysop Slug configured her system to automatically store messages, the interception and disclosure of the contents of the electronic communications would fall beyond the peripheral protection of the ECPA since the ECPA only covers the interception of communications "while in transmission." One must also consider the bite of section 2515. According to that section, electronic communications cannot be suppressed.[131] Thus, Sysop Slug's disclosure to Eagle Eye would be authorized under the ECPA.

Greenwood would also seem to allow the admission of evidence surreptitiously retrieved from deleted files or messages once found in a "privte" chat room. Hackers would become the cyber-analog for the scavengers and snoops. The deletion of a message or a file would serve as the functional equivalent to taking out the garbage. If the government visited a site and undeleted a file, the "owner" of that file could not have a legitimate expectation of privacy in it under the analysis of *Greenwood*.

Under the combined analysis of *Katz* and *Hoffa*, Stoney and Talley's conversation would probably be treated as if they voluntarily disclosed information to a third party because of the societal understanding concerning sysop control. The system operator could not be considered the functional equivalent of the telephone operator depicted in *Katz*. Whereas society understands that Ma Bell will not listen in on our phone conversations, the same cannot be said about system operators. Because of the growing fear amongst system operators concerning government raids, they have eliminated or severely curtailed user privacy.[132] Ergo, the telephone and system operators are not the clear analogs one might think they are. This leads us to an unsavory sort of conclusion: police could illegally search and seize the system operator's stored data and use it against the system operator's users—not the system operator herself. Such reasoning would be in tune with the idea that "'Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.'"[133] Stoney and Talley are not the "victims" of the illegal search, Sysop Slug (under Fourth Amendment jurisprudence) is the only real victim.

Even laws which curb the system operator's ability to monitor a user's communications would not, under the logic of *Greenwood* and *Oliver*, bear

131. *See* discussion *supra* Part II.E.
132. *Id.*
133. *Rakas*, 439 U.S. at 133–134.

on whether one has a reasonable expectation of privacy for purposes of standing jurisprudence under the Fourth Amendment.[134] Although the ECPA provides for civil remedies under section 2520 for certain system operator conduct which violates a user's privacy, *Greenwood's* rationale would seem to lend credence to the argument that the ECPA could not provide an individual with the legitimate expectation of privacy needed for standing. In cyberspace this argument becomes even stronger upon analogizing from *Greenwood.* The Court in *Greenwood* found that a state statute provided for the use of the exclusionary rule when police illegally searched garbage.[135] In the case of cyberspace and system operators, we are only dealing with a statute which provides for civil remedies when the proscribed conduct arises.[136] Further, the use of the exclusionary rule does not seem to apply to electronic communications under the section 2515 and the basic canon of *expressio unius.*[137] If the statute in *Greenwood* would not provide a basis for a legitimate expectation of privacy, a statute which dealt specifically with the exclusion of evidence, then it is a small step in logic to argue that the civil remedies set forth in section 2520 will not be sufficient insofar as one's reasonable expectation of privacy is concerned. This argument is buttressed by the fact that the exclusion of "electronic communications" is not provided for in section 2515.

C. *Electronic Mail*

Stoney and Talley, now in separate jail cells awaiting trial, suffer extreme withdrawal symptoms as they are without their portable laptops and each other. Luckily for them, the kind-hearted and dim-witted Nurse Hatchet takes pity on the two inmates and buys them both portable laptops equipped with cellular modems.

Behind steel bars and beneath prison issued blankets, electronic illuminesence brings smiles to the faces of Stoney and Talley. Being careful not to enter into any sort of chat room, they dial into their "private" e-mail accounts on Casablanca Online ("COL"), the largest public online service in the United States.

---

134. Although the ECPA provides civil remedies for certain system operator conduct which violates a user's privacy, under the logic of *Greenwood* and *Oliver*, the ECPA could not provide an individual with a legitimate expectation of privacy. *See supra* notes 94–101 and accompanying text.

135. *Greenwood*, 486 U.S. at 43–44.

136. *See* 18 U.S.C. § 2520.

137. *See* discussion *supra* Part II.E.

After entering in their passwords, each send detailed accounts of their plan to break out of prison (which eclipse mere preparation and rise to the level of perpetration under the law of criminal attempts) and take over cyberspace. Other than the sysop, no one can access their e-mail accounts.

Stoney promised to advertise for COL in exchange for its promise not to disclose any e-mail to anyone unless a properly executed search warrant forced it to do so. Stoney and COL signed a legally binding contract evidencing their promises. Talley was too lazy to make a similar contract with COL.

With a gun and a smile, Officer McFadden asked the COL system operator to turn over any messages stored in Stoney and Talley's e-mail accounts. McFadden arrests Stoney and Talley and again they move to suppress evidence at a pre-trial hearing.

As ridiculous as the above hypothetical is, the issue of standing remains a difficult one. Do individuals have a legitimate expectation of privacy in their e-mail accounts? While Officer McFadden certainly violated several laws in the pursuit of the e-mail, Stoney and Talley must have standing to assert the illegality of McFadden's actions. Though the exclusionary rule is designed to deter police misconduct,[138] standing remains a prerequisite for a motion to suppress evidence.[139]

Do Stoney and Talley have standing to suppress their e-mail messages? Under *Katz* and its progeny, both need subjective and objective expectations of privacy. On a subjective level, it would probably be difficult to show that neither had an actual expectation of privacy. This is especially true for Stoney who contracted with COL for the express purpose of ensuring his privacy. Is their expectation of privacy one which society is prepared to recognize as reasonable? Both Stoney and Talley evidenced indicia of control and the power to exclude with the use of their password. The password could be thought of as the functional equivalent of the key in *Jones* which the Court found to be very significant. However, unlike *Jones*, Stoney and Talley "voluntarily disclosed" the contents of their e-mail to the sysop by virtue of the societal understanding concerning the sysop/user relationship. Any possessory interest one might have in their e-mail is contingent on what the sysop decides to do with it. Thus, the power to exclude, traditionally linked to property rights, is tenuous at best in the context of e-mail communications. A legitimate expectation of privacy in this instance will

138. DRESSLER, *supra* note 5, at 239.
139. *See generally id.* at 219.

not flow from the possessory interest Stoney and Talley have in their communications.

The contract Stoney had with COL is rendered meaningless under the logic of *Hoffa, Greenwood,* and *Oliver.* The Fourth Amendment simply does not provide protection for a wrongdoers misplaced belief in the trustworthiness of a third party.[140] A contract, like a law or statute, will not create a legitimate expectation of privacy.[141] Stoney may try to sue COL for breach of contract (though COL would have a solid duress defense), but that would be his only mechanism for relief. The fact that Officer McFadden grossly violated COL's rights is of no concern. "'Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.'"[142]

On the other hand, Stoney might try to argue that his contract with COL provided him with a legitimate expectation of privacy similar to that which a tenant would have with his or her landlord.[143] Like a tenant or hotel guest, a user who has a present possessory interest in the e-mail would have standing to assert the illegality of a government search. Like the landlord-tenant relationship, a system operator may not effectively consent to the search of his user's e-mail communications. In fact, Stoney's contract with COL explicitly states that COL may not divulge the contents of e-mail unless the sysop is provided with a properly executed search warrant. Stoney may contend that such a contract is the functional equivalent of the implicit agreements between a landlord and her tenant, or a hotel and its guest, to not let others in their homes or rooms. Therefore, such a contract would provide Stoney with standing.

On the surface, this argument seems to be pretty convincing. However, implicit within such an argument is the proposition that the sysop/user relationship is analogous to the landlord-tenant relationship. In a landlord-tenant relationship (or hotel-guest relationship) the government searches homes or rooms. In cyberspace, the government searches for electronic data stored in the sysop's computer. The difference in the place searched might prove to be important. First, the Fourth Amendment traditionally has been interpreted to afford the greatest protection to the home and similar dwell-

140. *Hoffa*, 385 U.S. at 302.

141. *See Greenwood*, 486 U.S. at 43; Oliver v. United States, 466 U.S. 170 (1984); *see also supra* note 94–101 and accompanying text.

142. *Rakas*, 439 U.S. at 133–34 (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)).

143. Stoney might also argue that his situation is like that of the relationship between a hotel/motel guest and manager. *See* discussion *supra* Part II.C.

ings such as a hotel room.[144] Can the storage area where electronic information is kept logically be equated to a home? The type of activity which occurs at an e-mail address is distinct from the intimate activity which occurs at one's home (or hotel room). Second, a system operator may monitor *all* activities associated with the e-mail address after they are stored in her computer.[145] Conversely, a landlord or hotel manager cannot monitor the activities of her tenant or guest without some sort of contract allowing such monitoring. Clearly, the sysop's ability to monitor a user's e-mail severely curtails any legitimate expectation of privacy. This second level of differentiation would probably lead a court to conclude that a defendant in such a situation would not have standing despite any contract. There is little reason to think that electronic mail will be treated any differently from "private" chat rooms.

D. *The System Operator*

In addition to communicating via e-mail that day, Stoney and Talley decided to open up their own web-site and e-mail service. In order to access their sites, a person needed a password and rejection letter from the Cyber Law Center. As system operators, Stoney and Talley had complete dominion and control over the accessibility of their site.

Officer McFadden surreptitiously hacks into Stoney and Talley's web site and discovers pictures evidencing child pornography and bestiality in violation of state law. Stoney and Talley move to suppress the evidence as a violation of their Fourth Amendment rights.

Here, Stoney and Talley would have standing to assert the illegality of the search. They have a possessory interest in the website and the computer which they share with no one else. The password protection evidences self-protective steps which would rise to a legitimate expectation of privacy in this example because no one else aside from Stoney and Talley can circumvent the password to glean information from their web-site.[146] Because Stoney and Talley can choose who enters their site, they seem to have the

144. *See* Boyd v. United States, 116 U.S. 616 (1886) (explaining the historical backdrop for Fourth Amendment jurisprudence).

145. *See supra* notes 108–11 and accompanying text.

146. One might question the truth of this statement considering that McFadden hacked into Stoney and Talley's website. The difference here lies in the fact that the garbage was not taken to the curbside. *Greenwood* is taken out of the equation, assuming files are not deleted into Cyberspace. Here, it is unlikely that e-mail will be deleted into Cyberspace. Any deletion should remain within the physical confines of the computer. *See supra* notes 94–101, accompanying text, and discussion in Part IV.B.

power to exclude which is important in attaining a legitimate expectation of privacy. Stoney and Talley, as sysops, are direct victims of the illegal search. Thus, system operators seemingly would have standing to assert the illegality of police action when they take the self-protective steps required under the Fourth Amendment.

E. *Pen Register and Beeper Analogies*

Hypothetically, if the police used a device to track where one travels in cyberspace, there is no reason to think that the use of such technology would constitute a search under the Fourth Amendment. When one travels along the digital highway, such movements are knowingly exposed to the public and merit no Fourth Amendment protection. The digital web where a user journeys would be considered the functional equivalent of the public streets. A cyber-beeper[147] or pen register would seem to comport with the Court's analysis in *Smith* and *Knotts*. As long as a user travels along a *public* area in cyberspace, where one can legally view their movements, cyber-tracking devices would not constitute a search.

F. *Data Encryption*

While searching through the records of Stoney and Talley's conversations in the public chat room at Worms R' Us, Officer McFadden discovers several lines of garbled text sent between Stoney and Talley. Stoney and Talley encrypted the most detailed portions of their plan to destroy the Cyber Law Center. Presently, there is no method to decrypt a message unless one has the key to decode it. Stoney and Talley each memorized the keys and have never written them down.

Encryption of data is the only surefire way to ensure privacy.[148] Only those who have the key can decrypt an encoded message. Encrypted data acts like an impenetrable bomb shelter. Nothing can break into it. It would seem that the power to exclude others with this technology is absolute. That being the case, it would seem one will always have standing to challenge the illegality of a search or seizure of encrypted data. By definition, it is taken out of the public view.

For every rule there is an exception. The United States government created encryption software called the "Clipper."[149] Those who use Clipper

147. A cyber-beeper is a hypothetical label that this author is attaching to a device used to track movement in cyberspace.

148. NETLAW, *supra* note 102, at 181–85.

149. *Id* at 182.

encryption must be aware that the government holds the keys for decryption in escrow with government agencies.[150] This factor would diminish one's legitimate expectation of privacy. Further, if technology becomes available to the public which would allow one to decrypt at will, then encryption will become obsolete as a means for ensuring a legitimate expectation of privacy under the rationale of *Dow Chemical.*

V. CONCLUSION

Based upon the above analysis, it would seem that encryption of data is the only way a *user* can attain a legitimate expectation of privacy for purposes of standing under the Fourth Amendment. The *system operator* can gain a legitimate expectation of privacy in cyberspace, but she must take adequate self-protective steps equivalent to those outlined in *Katz* and its progeny. Thus, the criminal defense attorney should advise her clients not to store any information in cyberspace unless they would be willing to shout out the same information in a crowded public theater.

"He looked up again at the portrait of Big Brother. The colossus that bestr[ides] the world!"[151]

Brian I. Simon[*]

---

150. *Id.*

151. GEORGE ORWELL, 1984 at 244 (NAL Penguin Inc. 1961). In Erich Fromm's afterword to *1984,* he crystallized the impetus this author had for altering the tense in one of the last passages George Orwell wrote in *1984.*

> George Orwell's *1984* is the expression of a mood, and it is a warning. The mood it expresses is that of near despair about the future of man, and the warning is that unless the *course of history* changes, men all over the world will lose their most human qualities, will become soulless automatons, and will not even be aware of it.

Erich Fromm, *Afterword* to GEORGE ORWELL, 1984 (NAL Penguin Inc. 1961) (emphasis added).

Unless the current state of the law changes (§ 2515 of the ECPA should be considered a prime candidate for change), and the courts and Congress act with a keen eye toward learning about the Internet, it is this author's opinion that that we will forever remain stuck in a sand trap throughout the "course of history."

* The author would like to thank Professors Johnny C. Burris and Mark Dobson of the Nova Southeastern University, Shepard Broad Law Center for their insight, support, and assistance in helping prepare this article for publication. Please send e-mail comments to the author at <simonbr@law.acast.nova.edu>.