Volume 8, Number 1 Fall 1994

SEARCHES AND SEIZURES OF COMPUTERS AND COMPUTER DATA

*Raphael Winick**

INTRODUCTION

In 1928, Justice Brandeis predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[1]

Technological developments have turned Justice Brandeis' foresighted prediction into reality. One man has been sentenced to death in a kidnapping and murder case following the electronic recovery by police of ransom notes which had been previously deleted from computer disks.[2] Government monitoring of a college student's electronic bulletin board and Internet site resulted in a recent felony indictment on fraud and software piracy charges.[3] Incriminating electronic mail messages led to pending criminal charges for theft of trade secrets against high-ranking executives at software giants Symantec and Borland.[4] A 1990 FBI and Secret Service seizure of computer hardware and software from a Texas distributor of computer-related literature deprived the publisher of documents necessary to complete several books and other projects,

---

* J.D., Duke University, 1992; B.A., Brown University, 1988. The author is an associate with the New York office of Latham & Watkins.

1. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967). Although Justice Brandeis wrote these words in dissent, the Court later accepted his position and overruled the *Olmstead* majority opinion in *Katz*.

2. Commonwealth v. Copenhefer, 587 A.2d 1353 (Pa. 1991).

3. Peter H. Lewis, *Student Accused of Running Network for Pirated Software*, N.Y. TIMES, Apr. 9, 1994, at A1.

4. John Markoff, *2 Executives Indicted in Trade-Secret Theft*, N.Y. TIMES, Mar. 5, 1993, at D3; *see also* Siemens Solar Indus. v. Atlantic Richfield Co., No. 93 Civ. 1126 (LAP), 1994 WL 86368 (S.D.N.Y. Mar. 16, 1994) ($150 million securities suit filed in federal court based on incriminating electronic mail messages).

thereby threatening the viability of that company.[5] The R.J. Reynolds Tobacco Company has subpoenaed an anti-smoking computer bulletin board service to produce its membership list.[6] Due to public concern over civil liberties the federal government announced in the summer of 1994 that it will reevaluate controversial plans to create a federally-designed and governmentally-controlled standard for encrypting electronic transmissions.[7]

Americans' growing reliance on computers has vastly increased the potential for the government to use electronic surveillance to intrude into its citizens' private lives. Individuals are losing the ability to physically lock away sensitive information from curious eyes.[8] Justice Douglas once noted: "Electronic surveillance is the greatest leveler of human privacy ever known. . . . [E]very person is the victim, for the technology we exalt today is everyman's master."[9] Chief Justice Warren shared this fear: "[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; [the] indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments."[10]

Computers are fast becoming a primary method of storing personal information and transmitting private communications. Criminal enterprises have followed legitimate businesses in utilizing computers to store records, execute transactions, and communicate with others. Law enforcement agencies have reacted to these developments by directing their attention toward the use of computers in criminal enterprises and the possibility that computers may contain evidence of illegal activity. Local and federal agencies now frequently utilize evidence garnered from computers to build their cases and use their own computers as offensive weapons to detect criminal activity. The government's reaction to the information age will likely raise the most important issues of personal privacy this country will face in the next several decades.

Searches and seizures of computers and computer data present

---

5. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

6. Peter H. Stone, *Smoking Out The Opposition*, 26 NAT'L J. 925, Apr. 16, 1994.

7. Elizabeth Corcoran & John Mintz, *Administration Steps Back on Computer Surveillance*, WASH. POST, July 21, 1994, at A1.

8. *See* S. REP. NO. 541, 99th Cong., 2d Sess. 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

9. United States v. White, 401 U.S. 745, 756-57 (1971) (Douglas, J., dissenting).

10. Lopez v. United States, 373 U.S. 427, 441 (1963) (Warren, C.J., concurring).

complex legal questions that, if resolved incorrectly, present a very real threat of massive intrusions into civil liberties. Several instances of abuse have already been documented.[11] Constitutional scholars, industry professionals, and civil libertarians have all expressed fears that existing law fails sufficiently to safeguard our privacy. Harvard law professor Laurence Tribe has even called for the proposal and passage of a constitutional amendment specifically protecting the privacy of electronic communications.[12]

This article discusses the statutory and constitutional provisions protecting the privacy of stored or transmitted computer data. Part I offers a general review of the statutory and constitutional protections currently applied to electronically stored data, concluding that a high expectation of privacy will attach to such data under these provisions. Part II discusses the extent to which these existing provisions protect stand-alone computer systems, and advocates that courts and law enforcement personnel apply the Ninth Circuit's "intermingled documents" rule to determine the permissible scope of searches and seizures of computers. Part II also discusses issues related to the encryption of computer files and the return of computer equipment after its seizure. Part III analyzes the protection offered to on-line systems and electronic bulletin board systems ("BBSs") by the Electronic Communications Privacy Act and by the Privacy Protection Act. Part III also analyzes the special situation presented by computer systems that contain political or sexual subject matter.[13]

---

11. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994); Editorial, *Search and Seizure, Computer Style*, ST. LOUIS POST-DISPATCH, Jan. 26, 1993, at 2C (FBI seized computer bulletin board system in search for pornographic files, leading to losses of $40,000 for the owner of the system, who had consistently tried to keep pornographic material off the system and had kept the local police notified of pornographic materials transmitted on his system); BRUCE STERLING, THE HACKER CRACKDOWN (1992) (a full-length book discussing government raids on suspected computer hackers).

12. Paul Freiberger, *Computer-Age Call for New Amendment*, CHI. TRIB., Mar. 31, 1991, at 2; *see* Matthew Goldsmith, *Privacy Laws Urged for Data Superhighway*, N.Y. L.J., Jan. 24, 1994, at 1 (discussion of legislative proposals and calls for increased protection).

13. The issues surrounding an employer's ability to monitor an employee's computer use and electronic mail have generated significant discussion in the legal literature. For in-depth discussions of this issue, see David Neil King, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap,"* 67 S. CAL. L. REV. 441 (1994); Steven Winters, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197 (1993); Lois R. Witt, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?*, 96 DICK. L. REV. 545 (1992); Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop*, 41 DEPAUL L. REV. 739 (1992); Steven B. Winters, *Do Not Fold, Spindle or Mutilate: An Examination of Workplace*

Examination of the relevant statutes and case law demonstrates that adequate protection of electronic data is possible under existing constitutional and statutory authority. The Fourth Amendment, the Electronic Communications Privacy Act, and the Privacy Protection Act provide a solid framework within which the privacy of electronic data can be protected. Although only a handful of published cases deal specifically with computer data, the few relevant cases indicate that courts recognize the important privacy interests implicated by searches and seizures of computer data. However, these cases resolve few of the key issues. Adequate protection will develop only if the courts extend existing constitutional and statutory principles with an understanding of the intangible nature of computer storage, and an appreciation that the massive storage capacity of modern computers creates a high risk of overbroad, wide-ranging searches and seizures.

I. CONSTITUTIONAL AND STATUTORY LIMITATIONS ON SEARCHES AND SEIZURES

The Fourth Amendment and two little-known federal statutes ensure all Americans some protection from unwanted searches and seizures. The Fourth Amendment remains the most robust source of general protection. One federal statute, the Electronic Communications Privacy Act, applies explicitly to searches of computers, while a second statute, the Privacy Protection Act, by its plain language appears to apply to electronic bulletin boards and other on-line computer systems. Both statutes exceed the constitutional protections of the Fourth Amendment in several ways. Additionally, some state constitutional and statutory provisions supplement the federal protections.

A. The Fourth Amendment and Surrounding Case Law

With the possible exception of the First Amendment, the Fourth Amendment provides the most important constitutional protection against

---

(1992); Steven B. Winters, *Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail*, 1 S. CAL. INTERDISC. L.J. 85 (1992); Michael W. Droke, *Private, Legislative and Judicial Options for Clarification of Employee Rights to the Contents of Their Electronic Mail Systems*, 32 SANTA CLARA L. REV. 167 (1992); Jennifer J. Griffin, *The Monitoring of Electronic Mail in the Private Sector Workplace: An Electronic Assault on Employee Privacy Rights*, 4 SOFTWARE L.J. 493 (1991).

governmental intrusion into personal matters. The amendment provides that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[14] Like other provisions of the Bill of Rights, the Fourth Amendment "limit[s] . . . the power of the sovereign [state] to infringe on the liberty of the citizen."[15]

The Fourth Amendment protects individuals, corporations,[16] and other entities from government-sponsored monitoring of their activities. The framers "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man."[17] The Supreme Court has explicitly recognized that the Fourth Amendment, with its warrant requirement and court-supplied exclusionary rule, exists because the self-restraint of law enforcement authorities provides an insufficient safeguard against invasions of privacy.[18]

The Fourth Amendment prohibits only unreasonable *government* searches and seizures; it does not apply to searches conducted by private parties unconnected with government activities. Consequently, private searches implicate the Fourth Amendment only when they are conducted with both the knowledge of law enforcement authorities and with the intent to assist those authorities.[19] The Fourth Amendment therefore provides no protection against the actions of private citizens who, without the knowledge, encouragement or participation of government authorities, monitor electronic communications or gain access to confidential information stored on a computer. This restriction holds true even if the private citizen later turns the information over to the government.[20]

---

14. U.S. CONST. amend. IV.

15. Meachum v. Fano, 427 U.S. 215, 230 (1976) (Stevens, J., dissenting).

16. General Motors Leasing Corp. v. United States, 429 U.S. 338, 353 (1977) (stating that corporations enjoy some Fourth Amendment protection).

17. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

18. *See* United States v. United States Dist. Court, 407 U.S. 297, 316-17 (1972).

19. *See* United States v. McAllister, 18 F.3d 1412, 1417 (7th Cir. 1994); United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1993); Pleasant v. Lovell, 974 F.2d 1222, 1226 (10th Cir. 1992).

20. *See McAllister*, 18 F.3d at 1418; United States v. Attson, 900 F.2d 1427, 1432 (9th Cir. 1990).

The Supreme Court employs two key procedural devices to realize the protections guaranteed by the Fourth Amendment: the warrant requirement and the exclusionary rule. Generally, law enforcement authorities must obtain a warrant from a neutral magistrate before searching a place in which an individual has an objectively reasonable expectation of privacy.[21] The warrant must be supported by probable cause to believe that evidence of unlawful activity will be discovered, and must particularly describe the place to be searched and the things to be seized.[22] However, the warrant requirement admits many exceptions, most of which serve to protect the well-being of law enforcement officers or to preserve evidence from destruction.[23]

The Fourth Amendment derives much of its power from the exclusionary rule, which, as first enunciated by the Court in 1914,[24] provides that if law enforcement officials engage in an unlawful search or seizure, none of the fruits of that search may be used in subsequent prosecutions. The tainted and inadmissible "fruit of the poisonous tree" includes evidence seized in an unlawful search, additional warrants obtained in reliance on such searches, and all resulting evidence.[25]

Fourth Amendment inquiry ultimately centers upon whether a search or seizure is "reasonable." This reasonableness inquiry has been further refined into an initial two-prong test: first, does an individual have a subjective expectation of privacy in the thing searched or seized; and second, is society prepared to accept that expectation as objectively reasonable.[26] Case law reveals general principles that help clarify the amorphous concept of a "reasonable expectation of privacy." One line of cases holds that the Fourth Amendment protects certain areas of individual activity more highly than others, while another establishes that certain government activities are considered less intrusive into personal privacy.

The cases delineating protected areas of individual activity indicate that computer data will be entitled to a very high level of protection. The plain language of the Fourth Amendment protects "persons, houses, papers,

---

21. The various opinions generated in California v. Acevedo, 500 U.S. 565 (1991), contain comprehensive discussions of the origin and development of the warrant requirement, with Justice Scalia's concurring opinion noting that the Fourth Amendment does not include a warrant "requirement" within its plain language.

22. Dalia v. United States, 441 U.S. 238, 255 (1979).

23. *See Acevedo*, 500 U.S. at 581-85 (Scalia, J., concurring).

24. *See* Weeks v. United States, 232 U.S. 383, 398 (1914).

25. Wong Sun v. United States, 371 U.S. 471, 485-86 (1963).

26. California v. Greenwood, 486 U.S. 35, 39 (1988) (citing O'Connor v. Ortega, 480 U.S. 709, 715 (1987)).

and effects."[27] Given this language, courts universally hold that repositories of personal effects and information enjoy the highest level of Fourth Amendment protection.[28] The intangible nature of computer data does not affect the analysis, since the Court has long recognized that the Fourth Amendment protects "intangible as well as tangible evidence."[29]

Since computers are repositories of personal information, they will enjoy strong protection under the Fourth Amendment. The variety of information commonly stored on a computer, and the enormous and ever-expanding storage capacity of even simple home computers, justifies the highest expectation of privacy. As courts are beginning to discover, modern computers contain massive quantities of data relating to all aspects of an individual's or a corporation's activities. A typical home computer with a modest 100-megabyte storage capacity can contain the equivalent of more than 100,000 typewritten pages of information. This information can include business and personal documents, financial records, address and phone lists, and electronic mail communications.[30] Corporate computer systems have even more massive capacities, which corporations and their employees use to store a wide variety of information.

Although only a handful of reported decisions directly discuss the expectation of privacy in computer memory, these opinions agree that stored computer memory enjoys a very high level of constitutional protection. In three cases involving information stored electronically in the computer memory of display-type telephone pagers, federal courts in California, Nevada and Wisconsin stated this proposition vigorously. In *United States v. Chan*, the district court stated that "the expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information,"[31] and that "an individual has the same expectation of privacy in a pager, computer or other electronic data storage and retrieval device as

27. U.S. CONST. amend. IV.

28. United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992) ("Common experience of life . . . surely teaches all of us that the law's 'enclosed spaces'—mankind's valises, suitcases, footlockers, strong boxes, etc.—are frequently the objects of his highest privacy expectations.") (quoting United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)).

29. Warden v. Hayden, 387 U.S. 294, 305 (1967) (citing *Wong Sun*, 371 U.S. at 485-86).

30. *See* C. Ryan Reetz, *Warrant Requirement for Searches of Computerized Information*, 67 B.U. L. REV. 179, 191-92 nn.103-07 (1987) (discussing the variety of information stored on typical home and office computers); Terri Cutrera, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 U. MO. KAN. CITY L. REV. 139, 160 nn.198-99 (1991) (same).

31. 830 F. Supp. 531, 534 (N.D. Cal. 1993).

in a closed container."[32]

Closed containers likely to store personal information may be searched only when the search is authorized by a valid warrant, or when some exigent circumstance justifies a warrantless search.[33] However, analogizing stored computer memory to a closed container presents several problems. The container model may make conceptual sense when discussing small electronic storage devices such as pagers or electronic address books, but the analogy becomes strained when applied to computers with larger storage capacities. For such systems, an analogy to a massive file cabinet, or even to an entire archive or record center, may be more appropriate.

Recently, a federal district court in New York embraced the file cabinet analogy instead of the container analogy. In *In re Subpoena Duces Tecum*,[34] the court quashed on the grounds of overbreadth a grand jury subpoena for a company's hard disk. The court noted that although the disk might contain incriminating information, the hard disk also contained highly personal files, such as a draft of a will and personal financial information.[35] As discussed in part II.C, *infra*, the conceptual differences between a file cabinet and a container create an important distinction in establishing the appropriate scope of a search. Regardless of whether courts analogize computer storage to a file cabinet or to a container, either analogy leads to the conclusion that the information stored on a computer enjoys strong Fourth Amendment protection.

The location of a particular computer outside of one's home does not eliminate the high level of protection accorded to the contents of that computer. Although repositories of personal information are most likely to be found in one's home, cases involving the contents of office file cabinets,[36] luggage,[37] and briefcases[38] establish that personal information

---

32. *Id.* at 535 (quoting United States v. Blas, No. 90-CR-162, 1990 WL 265179 (E.D. Wis. Dec. 4, 1990)); *see also* United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (stating that in its capacity to store information, computer memory "is indistinguishable from any other closed container, and is entitled to the same Fourth Amendment protection") (citing Robbins v. California, 453 U.S. 420, 427 (1981)). Although appellate courts have *upheld* some searches and seizures of computer memory devices, these courts have all relied on an individual's lack of standing to challenge the search, and have avoided indications that computer memory enjoys anything other than a very high level of protection. *See, e.g.*, United States v. Lyons, 992 F.2d 1029, 1031-32 (10th Cir. 1993); United States v. Meriwether, 917 F.2d 955, 958-59 (6th Cir. 1990).

33. United States v. Bosby, 675 F.2d 1174, 1180 (11th Cir. 1982).

34. 846 F. Supp. 11 (S.D.N.Y. 1994).

35. *Id.* at 12.

36. O'Connor v. Ortega, 480 U.S. 707, 718 (1987).

37. United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992); United States v.

and effects do not lose their protection merely because they are not located within one's home.

Users of multi-user computer systems are also entitled to vigorous Fourth Amendment protection. Although in such systems users do not own the hardware, they nevertheless maintain an expectation of privacy in the information stored on the system. In order to maintain a legally cognizable expectation of privacy, an individual must have some possessory interest in the items searched or seized.[39] However, a possessory interest does not require ownership.[40] An individual must generally only have some right to exclude others in order to establish the requisite property or possessory interest.[41] Depending on the specific nature of their use, renters, lessors and many types of authorized users can maintain an expectation of privacy in the object of a search or seizure.[42] Based on these existing Fourth Amendment principles, the authorized users of a computer system should be able to maintain an expectation of privacy in data and other information stored on the system, if they can show a property or possessory interest in the data, and a right to exclude others from accessing that data.

The Fourth Amendment protects computers from remote access as well as from physical invasions. Initially, courts understood the Fourth Amendment to protect individuals only from *physical* invasions of their persons, effects, or homes.[43] However, in a 1967 decision involving electronic eavesdropping, the Court held that the Fourth Amendment applied even where there was no physical invasion of a constitutionally protected area.[44]

Block, 590 F.2d 535, 541 (4th Cir. 1978).

38. United States v. Bosby, 675 F.2d 1174, 1180 (11th Cir. 1982).

39. Rakas v. Illinois, 439 U.S. 128, 149 (1978).

40. Katz v. United States, 389 U.S. 347, 352 (1967); Jones v. United States, 362 U.S. 257, 263-66 (1960).

41. United States v. Torch, 609 F.2d 1088, 1091 (4th Cir. 1979), *cert. denied*, 446 U.S. 957 (1980); *see Rakas*, 439 U.S. at 149.

42. Minnesota v. Olson, 495 U.S. 91, 95-100 (1990) (holding that an overnight guest had a reasonable expectation of privacy in the premises searched); United States v. Davis, 932 F.2d 752, 756-57 (9th Cir. 1991) (holding that a former tenant who retained a key and had free access to stored items in an apartment enjoyed a reasonable expectation of privacy in the apartment); United States v. Rettig, 589 F.2d 418, 423 (9th Cir. 1978) (holding that a defendant who paid a portion of the rent and had a key and access to an apartment had a sufficient possessory interest to confer standing to challenge the search, even though defendant lived elsewhere); United States v. Robinson, 430 F.2d 1141 (6th Cir. 1970) (holding that defendant could still challenge search despite long absence from premises).

43. Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

44. *See Katz*, 389 U.S. at 352.

A computer owner or user may lose her expectation of privacy in the contents of the computer's memory if she makes the computer generally accessible to others. Case law establishes that if an individual disclaims an exclusory interest in property, the individual forfeits any expectation of privacy in that property.[45] The property is then subject to lawful search or seizure by government officials.[46] As applied to computer networks and on-line systems, this doctrine implies that as one makes resources of a system increasingly available to others, the expectation of privacy one enjoys in those resources diminishes. This issue, and other issues related to searches of networks, on-line systems, and user accounts, are discussed in part III, *infra*.

In addition to losing an expectation of privacy by allowing general access to a computer system, an individual may lose an expectation of privacy in stored, but unprotected, information under the plain view doctrine, which holds that evidence placed in plain view no longer carries any expectation of privacy.[47] Extending this principle to computer communications implies that once someone places data or other evidence onto a computer in a publicly-accessible manner, they lose any expectation of privacy in the information.[48]

Individuals can also lose the protection of the Fourth Amendment by disclosing information to another party. When someone voluntarily discloses information to another party, they do so at their own risk.[49] The receiving party may relay that information to law enforcement authorities without violating the Fourth Amendment.[50] Additionally, the Fourth Amendment permits the receiving party to electronically monitor or record the information disclosed, and then transfer the resulting electronic records to law enforcement authorities.[51] For example, in *United States v. Meriwether*, the defendant voluntarily transmitted his telephone number

---

45. *Cf.* California v. Hodari D., 499 U.S. 621, 624 (1991) (noting that a person who abandons property, for example by dropping it, loses all Fourth Amendment protection with respect to that property).

46. *Id.*

47. Horton v. California, 496 U.S. 128, 133-34 (1990).

48. *See infra* part III.A, B.

49. Hoffa v. United States, 385 U.S. 293 (1966).

50. United States v. White, 401 U.S. 745 (1971) (holding that government monitoring of conversations between the defendant and an informant, by a radio transmitter concealed on informant, does not violate the Fourth Amendment).

51. United States v. Seidlitz, 589 F.2d 152, 158-59 (4th Cir. 1978) (holding that since the operator of the computer system, rather than a government agent, performed the search, the government may use results from the tracing of phone calls and electronic recordings of unauthorized activity on a corporate computer system).

and a secret numerical code to an electronic pager, hoping to arrange a cocaine deal.[52] Unknown to the defendant, the Drug Enforcement Agency had confiscated the pager after arresting its owner. In order to arrange a cocaine transaction, the DEA called the telephone number which had been sent by the defendant and electronically recorded within the pager. The Sixth Circuit rejected the defendant's claim that the DEA's seizure of the defendant's phone message stored in the pager's memory violated the Fourth Amendment, reasoning that the defendant had "no legitimate expectation of privacy in information he voluntarily turns over to third parties."[53]

Computer users therefore transmit electronic mail and other communications at the risk that the recipient may divulge the contents to law enforcement authorities. A more difficult problem is whether operators of networks, on-line systems, and electronic mail systems may monitor transmissions, and then relay any pertinent information to the government. In the only reported case on point, the Fourth Circuit held that the operator of a corporate computer system was a party to computer transmissions, and therefore had the authority to trace unauthorized computer communications.[54] However, the Electronic Communications Privacy Act of 1986 ("ECPA"),[55] enacted several years after the Fourth Circuit's decision, has superseded *Seidlitz* as applied to computer communications affecting interstate commerce. The ECPA regulates the ability of owners or operators of computer networks to monitor the communications of the systems' users, prohibiting the random monitoring by service providers of the contents of computer communications.[56]

If a computer is searched or seized under a valid warrant, a suspect can still challenge the *scope* of the search or seizure. Two Fourth Amendment doctrines require suppression of the fruits of a search or seizure if the scope is impermissibly broad. First, the particularity requirement mandates that a warrant must particularly describe the object to be searched and the things to be seized.[57] Second, the overbreadth

52. 917 F.2d 955 (6th Cir. 1990).

53. *Id.* at 959 (citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

54. *Seidlitz*, 589 F.2d at 158 (holding that the operator of a computer system had the authority to trace unauthorized downloading of source code from corporate computer system).

55. Title I of the ECPA is codified at 18 U.S.C. § 2510 *et seq.* (1988). Title II of the ECPA is codified at 18 U.S.C. § 2701 *et seq.* (1988).

56. For a detailed discussion of the ECPA, see *infra* part I.B.

57. Maryland v. Garrison, 480 U.S. 79, 84 (1987).

doctrine limits the scope of a search to the specific areas and things for which there is probable cause to search.[58]

The particularity requirement ensures that a "search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[59] For example, search warrants that permit searches of "all records" of a business or an individual generally lack particularity.[60]

Seizures of computers and large hard disks have a high potential for becoming intrusive and impermissible "all records" searches. Given the massive storage capacities of disks and other modern storage media, a single disk may well contain information on a vast array of topics. For example, officers searching a computer for a telephone number may use the opportunity to rummage through financial records, written correspondence, electronic mail, or other obviously personal and irrelevant records also contained on the computer.

One recent decision recognized that a search of a large hard disk lacked particularity.[61] However, other cases indicate that individuals will have difficulty prevailing on particularity challenges to warrants authoriz-

---

58. *Id.* The particularity requirement and the overbreadth doctrine apply to some civil searches as well as to searches conducted as part of a criminal investigation. Court-authorized civil searches, seizures, and impoundments conducted under the copyright laws are guided by the Fourth Amendment principles of particularity and probable cause. *See* Paramount Pictures Corp. v. Doe, 821 F. Supp. 82, 90 (E.D.N.Y. 1993) (holding that civil plaintiff's proposed seizure order of allegedly pirated videotapes lacked particularity and was overbroad); First Technology Safety Sys., Inc. v. Depinet, 11 F.3d 641, 649-52 (6th Cir. 1993) (holding that an ex parte order for the seizure of computer records under the Copyright Act was invalid). This principle will help protect bulletin board operators from overbroad civil searches and seizures if the BBS is suspected of being used as a conduit for software piracy.

59. *Garrison*, 480 U.S. at 84. When officers exceed the scope of a warrant, only information discovered beyond the scope of the warrant is suppressed. United States v. Riggs, 690 F.2d 298, 300 (1st Cir. 1982).

60. *See* Naugle v. Witney, 755 F. Supp. 1504, 1515-16 (D. Utah 1990). In considering a civil charge of civil rights violations, the court held that the seizure of file cabinets and computers under a warrant calling for seizure of "all records . . . and computer hardware and software" was not specific as to the circumstances and the nature of the activity under investigation, and was therefore unconstitutionally overbroad. In a companion criminal case, the seized evidence was admitted under the plain view exception, after severing the invalid portions of the warrant. United States v. Naugle, 997 F.2d 819 (10th Cir. 1993), *cert. denied*, 114 S. Ct. 562 (1993). A warrant may authorize the seizure of all of the records of a business only when there is probable cause to believe that the business is engaged in a pervasive scheme to defraud and has no significant activities unrelated to the fraud. United States v. Falon, 959 F.2d 1143, 1146-48 (1st Cir. 1992); United States v. Kail, 804 F.2d 441, 444-45 (8th Cir. 1986); National City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980).

61. *See In re* Subpoena Duces Tecum, 846 F. Supp. 11, 13-14 (S.D.N.Y. 1994).

ing searches of computer memory. In *United States v. Hersch*, a Massachusetts federal district court upheld a seizure warrant for "all computer hardware, software, and related equipment" since "the complex scheme under investigation required seizure of the entire computer system in order to piece the scheme together."[62] In *United States v. Reyes*, the Tenth Circuit noted that business records are increasingly stored on magnetic media, and "in the age of modern technology and commercial availability of various forms of [storage media], the warrant could not be expected to describe with exactitude the precise form the records might take."[63] The same logic guided the Ninth Circuit in *United States v. Gomez-Soto*: "Failure of the warrant to anticipate the precise container in which the material sought might be found is not fatal."[64] Although neither *Reyes* nor *Gomez-Soto* involved computer storage devices, their logic suggests that a warrant providing merely for the search and seizure of "records" or "files" may be specific enough to encompass computer storage media, even if the warrant does not specify computer equipment.

Overbreadth is closely related to the particularity requirement. Two district court cases indicate that defendants will have difficulty sustaining overbreadth challenges to computer searches conducted under a warrant. In *United States v. Musson*, the court permitted the seizure of fifty-four computer diskettes under a search warrant specifying "correspondence, memoranda, . . . ledgers, . . . and any records and writings of whatsoever nature" detailing transactions of certain companies and individuals.[65]

An even more sweeping overbreadth decision is *United States v. Sissler*.[66] In *Sissler*, officers seized nearly 500 computer disks and a personal computer while executing a valid warrant permitting the search and seizure of "records of drug transactions, and records identifying marijuana customers and suppliers"[67] The court denied the defendant's motion to suppress the disks as the product of an overbroad search, reasoning that the police could search any container found on the premises if they reasonably believed that the container held the evidence sought

62. CR-A-93-10339-2, 1994 WL 568728, at *1 (D. Mass. Sept. 27, 1994).
63. 798 F.2d 380, 383 (10th Cir. 1986).
64. 723 F.2d 649, 655 (9th Cir.), *cert. denied*, 466 U.S. 977 (1984).
65. 650 F. Supp. 525, 531-32 (D. Colo. 1986).
66. No. 90-CR-12, 1991 WL 239000 (W.D. Mich. Aug. 30, 1991), *aff'd*, 966 F.2d 1455 (table), 1992 WL 126974 (6th Cir. 1992) (unpublished disposition), *cert. denied*, 113 S. Ct. 1004 (1993).
67. *Id.* at *2.

pursuant to the warrant.[68] The *Sissler* court noted that "the police were not obligated to give deference to the descriptive labels" on the disks, and that the disks could therefore all be seized.[69] More importantly, the court held that the police were not obligated to inspect the disks or the computer at the site of the search, since defeating passwords or other security devices on the computer might take some time and effort, and would best be performed off-site.[70]

These cases indicate that defendants will encounter difficulty succeeding on overbreadth and particularity challenges to searches of computer memory. Taken together, *Hersch*, *Sissler*, and *Musson* stand for the proposition that a warrant permitting a search of "records" permits officers to seize and search *all* computers and computer storage media, regardless of what "records" or "documents" are specified in the warrant. These holdings allow officers to rummage through all the stored data, regardless of what the labels or disk directories describe as the contents of the disks. However, the recent New York federal district court opinion in *In re Subpoena Duces Tecum*[71] takes a completely different approach, apparently creating an important division among the courts on the standards for evaluating potentially overbroad searches of computers.

In *In re Subpoena Duces Tecum*, the court quashed as overbroad a grand jury subpoena demanding the production of computer disks, where the prosecution conceded that the disks contained irrelevant information. The court reasoned that the subpoena should have specified certain categories of information, rather than merely specifying the method of storage.[72] According to the opinion, there was no need to subpoena the entire contents of the disks since a key word search could effectively separate relevant files from irrelevant files without surrendering the entire contents to the grand jury.[73]

Hersch, *Sissler*, *Musson*, and the other opinions permitting extremely broad searches of computer storage rely on a simplistic and inappropriate

---

68. *Id.* at *4 (citing United States v. Ross, 456 U.S. 798, 820-21 (1982)).
69. *Sissler*, 1991 WL 239000, at *4.
70. *Id.*
71. 846 F. Supp. 11 (S.D.N.Y. 1994).
72. *Id.* at 13-14.
73. *Id.* at 13. The fact that *In re Subpoena Duces Tecum* arose in the context of a grand jury subpoena, rather than in the context of a search warrant, should not limit its precedential value when applied to search warrants. As the court noted, the statutory "reasonableness" requirement of Fed. R. Crim. P. 17(c) governing the scope of grand jury subpoenas is the same as the "reasonableness" requirement of the Fourth Amendment. *Id.* at 12-13.

analogy between computers and closed containers. This analogy fails to recognize that Fourth Amendment closed container law developed in the context of searches of simple physical items stored in paper bags and suitcases, and that these simple items differ fundamentally from the massive quantities of intangible, digitally stored information residing on typical modern computers.[74] These fundamental qualitative and quantitative differences mandate a different analysis under the Fourth Amendment. These cases also ignore Fourth Amendment precedent that offers a special doctrine to cover the scope of searches for intermingled documents. This doctrine has been adopted or endorsed by courts and commentators who have directly addressed the question of intermingled documents, and is discussed in detail in part II.B, *infra*.

Once law enforcement officers lawfully seize computer data, attempts to defeat computer passwords, encryption, and other security techniques are permissible. Existing case law permits officers to use a variety of scientific and technological means to examine items seized under a warrant.[75] Given this principle, officers appear to be authorized to take all steps necessary to defeat computer security devices or encryption techniques. Encrypting data may make it more difficult for authorities to discover, locate, or understand stored information; however, encryption does not create any additional constitutional hurdles, and a separate warrant is not required to decrypt the information.

B. Statutory Protections

Two federal statutes protect the privacy of electronic data and communications. Since the protection offered by these statutes exceeds that afforded by the Fourth Amendment, a government action may be constitutionally acceptable, but still prohibited by these statutory requirements. Conversely, an action not expressly prohibited by statute may still be prohibited if it violates the constitution. Unlike the protections of the Fourth Amendment, these statutory prohibitions also apply to individuals not acting on behalf of the government.[76]

---

74. *See* discussion *infra* part II.B.

75. *See infra* note 188.

76. The Fourth Amendment, in contrast, prohibits only government activities. *See supra* notes 19-20.

1. The Electronic Communications Privacy Act of 1986 ("ECPA")[77]

The Electronic Communications Privacy Act of 1986 created the two most important statutory safeguards against unwanted searches of computer communications and data. Title I prohibits the unauthorized interception of electronic communications. Title II prohibits unauthorized access to stored electronic communications and data.

Congress specifically targeted the ECPA at "overzealous law enforcement agencies, industrial spies and private parties."[78] As a result, the ECPA protects many types of computer systems from unauthorized searches performed by private individuals, as well as protecting these systems from law enforcement officers. However, case law has not yet resolved several important interpretive questions.

a. Title I of the ECPA: Interception of Electronic Communications

Title I of the ECPA extends the federal wiretap law to prohibit the unauthorized interception of any wire or electronic communication.[79] Prior to enactment of the ECPA, the wiretap law protected only communications sent by common carrier that could be overheard and understood by the human ear.[80] The new law protects communications transmitted in inaudible, digital, or other electronic form, and does not require that communications be transmitted via common carrier.[81]

The ECPA protects transmissions of computer data under the new statutory category of "electronic communications,"[82] defined as those transmitted through copper wire, coaxial cable, fiber optic cable, microwave, or radio transmissions.[83] Protected digital transmissions include the computerized transfers of video, text, audio,[84] data, or "intelli-

---

77. Title I of the ECPA is codified at 18 U.S.C. § 2510 *et seq.* (1988). Title II of the ECPA is codified at 18 U.S.C. § 2701 *et seq.* (1988).

78. S. REP. No. 541, 99th Cong., 2d Sess. 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 [hereinafter ECPA Legis. Hist.].

79. *See* 18 U.S.C. § 2511(a)(1).

80. *Cf.* United States v. New York Tel. Co., 434 U.S. 159, 167 (1977) (upholding the use of pen registers to trace the telephone numbers of outgoing calls, in part because the information obtained was presented in visual, rather than aural form).

81. *See* ECPA, Pub. L. No. 99-508, Title I, § 101(a)(1)(C), 100 Stat. 1848, 1851 (1986) (codified at 18 U.S.C. § 2510 *et seq.*).

82. 18 U.S.C. § 2510(12).

83. The definition of electronic communications includes information "transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system." 18 U.S.C. § 2510(12).

84. Only digitized stored audio files fall within the definition of electronic communica-

gence of any nature."[85] There is no requirement that the communication make use of a common carrier, public telephone line, or any other public facility.[86] However, the ECPA protects only electronic communications "transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system *that affects interstate or foreign commerce.*"[87]

Courts have not explored the limits of the interstate commerce requirement under the ECPA. The communications themselves need not relate directly to interstate commerce.[88] The communications must merely be made on a system that affects interstate or foreign commerce.[89] Internet communications obviously fall within this definition, even if the recipient and sender are located in the same state. Nationwide networks, BBSs, and corporate computer systems that are linked over state lines also unambiguously fall within the scope of the statute. However, the definition becomes more ambiguous when considering computer networks that do not physically cross state lines.

The legislative history of the ECPA states explicitly that "private networks and intra-company communications systems are common today and brings them within the protection of the statute."[90] The legislative history also states that the ECPA protects the internal communications system of a corporation if the activities of the company affect interstate commerce.[91] If courts accept this expression of congressional intent, then the ECPA will protect the computer networks of corporations, universities, and other organizations, even if the computer system or the organization has no actual physical presence in more than one state, provided the activities of the organization affect interstate commerce.

If an electronic communication falls within the scope of the ECPA,

---

tions. Analog audio transmissions fall within the statutory definition of "wire communications." 18 U.S.C. § 2510(1). Encrypted or scrambled real-time voice conversations are included within the definition of "wire communications," but not within the definition of "electronic communications." ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3566. Computer generated voices are not considered oral or wire communications, but rather electronic communications. 18 U.S.C. § 2510(18); ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3570.

85. "'Electronic communications' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature." 18 U.S.C. § 2510(12).

86. *See* ECPA, Pub. L. No. 99-508, Title I, § 101(a)(1)(C), 100 Stat. 1848, 1851 (1986) (codified at 18 U.S.C. § 2510 *et seq.*).

87. 18 U.S.C. § 2510(12) (emphasis added).

88. *See* ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3565-66.

89. *See id.*

90. *Id.* at 3566.

91. *See id.*

law enforcement officials or private parties can generally intercept it only with prior judicial approval.[92] In order to obtain judicial approval, the applicant must demonstrate probable cause to believe that particular communications relating to a felony offense will be recovered through the interception.[93] In addition, the applicant must demonstrate why alternative methods of obtaining the information are inadequate.[94] The ECPA imposes strict minimization requirements on the scope and duration of the taps, which must "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."[95] Authorization is limited to the shortest duration necessary to achieve the objective of the interception, with a maximum duration of thirty days.[96] The statute contains an emergency exception to the requirement for prior judicial approval.[97] Emergency situations must involve a danger of immediate physical harm to a person, conspiratorial activities threatening national security, or activities characteristic of organized crime.[98] It appears that a threat of immediate danger to *property* cannot qualify for the emergency exception, unless it threatens national security.[99]

The ECPA does not provide for the automatic suppression of electronic communications intercepted in violation of the Act.[100] Although the wiretap statute provides that unlawfully intercepted wire or oral communications are automatically excluded from any future judicial proceedings, the statute does not similarly automatically exclude electronic communications. The lack of an automatic exclusionary rule under the ECPA for electronic communications is certainly troubling; it is difficult to discern any rational justification for the distinction between electronic communications on the one hand and oral or wire communications on the

---

92. *See* 18 U.S.C. §§ 2516, 2518; Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994). Federal prosecutors must seek approval from the Justice Department before even applying for a court order. UNITED STATES DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL, Title 9, § 7.114 (1993 Supp.).

93. *See* 18 U.S.C. § 2518(3).

94. *See* 18 U.S.C. § 2518(1)(c), (3)(c); *see also* United States v. Fernandez, No. 92-CR563, 1993 WL 88197 (S.D.N.Y. Mar. 25, 1993); discussion *infra* note 214.

95. 18 U.S.C. § 2518(5); *see* Scott v. United States, 436 U.S. 128, 140 (1978); *Steve Jackson Games*, 36 F.3d at 463.

96. *See* 18 U.S.C. § 2518(5).

97. *See* 18 U.S.C. § 2518(7).

98. *See id.*

99. *Id.*

100. 18 U.S.C. § 2518(10)(a); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 n.6 (5th Cir. 1994); United States. v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990). The ECPA does, however, provide for the suppression of *wire* communications that are stored electronically. *See* 18 U.S.C. § 2510(1).

other. However, evidence derived from electronic communications intercepted in violation of the ECPA may still be excluded by criminal defendants through two methods. First, many interceptions of electronic communications which violate the ECPA will also violate the Fourth Amendment, subjecting them to the Fourth Amendment's exclusionary rule. Second, the ECPA does permit "such preliminary and other equitable or declaratory relief as may be appropriate," which could include a suppression order.[101] The statute also provides for civil damages, including actual or statutory damages, punitive damages, and attorneys' fees.[102] However, money damages are clearly an inadequate remedy for a criminal defendant. In cases where the government has violated the ECPA but not the Fourth Amendment, courts should not hesitate to suppress the illegally obtained evidence. A failure to suppress this evidence would effectively condone the government's illegal search or seizure of electronic communications, eviscerating the effectiveness of the ECPA and threatening the privacy of all computer communications.

The ECPA also makes it illegal to manufacture, assemble, possess, or sell any device that is primarily useful for the surreptitious interception of electronic communications; however, government agents are exempt from this provision.[103] Software appears to fall within the conception of a "device" used to intercept computer communications.[104] The United States may demand forfeiture of interception devices.[105]

The statute protects only the contents of a communication, not the existence of a communication.[106] Under this provision, law enforcement agents can lawfully determine the identities of the computer systems that one accesses, and can monitor the recipients and sources of one's electronic mail, so long as the contents of the communications are not

---

101. 18 U.S.C. § 2520(b)(1).

102. Statutory damages are $100 a day for each violation, or $10,000, whichever is greater. 18 U.S.C. § 2520. The statutory language is ambiguous on the issue of whether the ECPA authorizes civil suits against local or federal government bodies, and courts have split on this issue. *Compare* Organizacion JD Ltda. v. United States Dep't of Justice, 25 F.3d 180 (2d Cir. 1994) (holding that the government may be held liable for damages under 18 U.S.C. § 2707(a)); PBA Local No. 38 v. Woodbridge Police Dep't, 832 F. Supp. 808, 823 (D.N.J. 1993) (same); Bodunde v. Parizer, No. 93 C 1464, 1993 WL 189941 (N.D. Ill. May 27, 1993) (same) *with* Amati v. City of Woodstock, 829 F. Supp. 998, 1001-03 (N.D. Ill. 1993) (collecting cases holding that the government may *not* be held liable for damages under the ECPA).

103. *See* 18 U.S.C. § 2512(1)(b), (2)(b).

104. *See* 18 U.S.C. § 2510(5).

105. *See* 18 U.S.C. § 2513.

106. *Cf.* 18 U.S.C. § 2510(8) (defining "contents").

intercepted.

The ECPA contains several limitations on its broad protections. The most important limitations are that: (1) The operator of an electronic communications system may monitor system communications if it suspects that the system is being misused, or if users explicitly or implicitly consent to monitoring; (2) Electronic communications are not protected if they are readily accessible to the public; (3) A system operator may divulge the contents of a communication if it inadvertently discovers incriminating information; (4) The system operator may divulge the contents of communications intercepted in the ordinary course of business.

Providers of electronic communication services may monitor the service when misuse is suspected.[107] However, service providers may not randomly monitor transmissions unless the monitoring is performed for mechanical or quality control purposes.[108] General monitoring by the system operator of the contents of electronic mail or other private communications therefore appears to be prohibited.

Only private communications are protected. The ECPA does not protect electronic communications readily accessible to the general public.[109] Unfortunately, the statute does not specifically define which electronic communications are readily accessible to the general public.[110] As discussed in part III.A of this article, many communications over BBSs are readily accessible to the general public and therefore unprotected. In addition, the ECPA does not protect electronic communications if one of the parties consents to the interception by law enforcement officials.[111]

The ECPA tolerates the inadvertent discovery of incriminating information by the operator of a computer system. When an electronic communications provider inadvertently obtains the contents of a transmission, and the communication appears to relate to the commission of an ongoing criminal activity, the provider may divulge the contents of the transmission to law enforcement agencies.[112]

---

107. *See* 18 U.S.C. § 2511(2)(a)(i); United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993), *cert. denied*, 113 S. Ct. 2997 (1993).

108. *See* 18 U.S.C. § 2511(2)(a)(i).

109. *See* 18 U.S.C. § 2511(2)(g)(i).

110. The statute does define "readily accessible to the general public" for radio communications. 18 U.S.C. § 2510(16).

111. *See* 18 U.S.C. § 2511(2)(c). Consent is invalid if the communication is intercepted for the purpose of committing a criminal or tortious act, including defamation. 18 U.S.C. § 2511(2)(d).

112. 18 U.S.C. § 2511(3)(b)(iv); ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N.

The ECPA also permits disclosure of the contents of a communication if it is intercepted in the ordinary course of business. Communications that are monitored by equipment provided by the service provider and used in the ordinary course of business are not considered to have been "intercepted" within the meaning of the ECPA.[113] The ordinary course of business exception has generated substantial controversy and confusion in wiretap cases. Application of this exception to the novel context of monitoring computers will continue to generate controversy as disputes arise over whether a service provider, employer, or user monitored the computer communications of others in the ordinary course of business.[114]

Title I of the ECPA applies only to interceptions of transmissions. Courts have held that when the government obtains *stored* transmissions and then plays them back, no interception within the meaning of the ECPA has occurred.[115] Although not protected by Title I of the ECPA, stored communications are still protected under Title II.

b. Title II of the ECPA: Stored Electronic Communications

Title II of the ECPA[116] protects stored electronic communications from unauthorized access. An individual or entity violates this portion of the ECPA by intentionally accessing or exceeding his authorization to use an electronic communication facility, and then obtaining, altering or preventing authorized access to a stored electronic communication.[117] Thus, a violation occurs merely by *accessing* an electronic communication system; the downloading of information or alteration of files is not required. Criminal penalties include up to two years in prison and a fine of up to $250,000. Civil penalties include injunctive relief, actual but not punitive damages, profits made by the violator as a result of the unauthorized access, and attorneys' fees.[118] In addition, an aggrieved party might seek a suppression order as part of the "preliminary and other

---

at 3580.

113. 18 U.S.C. § 2510(5)(a); ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3567.

114. *See infra* part III.A.

115. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994); United States v. Turk, 526 F.2d 654 (5th Cir.), *cert. denied*, 429 U.S. 823 (1976).

116. Title II of the ECPA is also known as the "Stored Wire and Electronic Communications and Transactional Records Act."

117. *See* 18 U.S.C. § 2701(a).

118. *See* 18 U.S.C. § 2707. Courts have not resolved the question of whether the ECPA authorizes civil suits for damages against government entities. *See supra* note 102.

equitable or declaratory relief as may be appropriate."[119] In establishing a violation of the act, a plaintiff need only show an intentional mens rea on the element of unauthorized access. The plaintiff need not demonstrate that there was any intent to obtain or alter records.[120]

As with Title I of the ECPA, the plain language of Title II does not completely resolve the question of which computer systems fall within its scope. The ECPA does not protect stand-alone systems. Computers must qualify as an "electronic communications system," "electronic communications service," or "remote computing service"[121] to fall within Title II. Title II defines remote computing services as those providing computer storage or processing services to the public by means of an electronic communications system. The definition of "electronic communications system" includes computer facilities used to store electronic communications.[122] As discussed previously, intra-company networks, BBSs, and other on-line systems unambiguously fall within these definitions, provided they satisfy the very broadly defined interstate commerce requirement.[123]

The most important provisions of Title II prohibit private citizens from gaining unauthorized access to stored electronic communications and enumerate specific procedural requirements for a government entity to gain access to stored electronic communications. Law enforcement authorities can access an electronic communication that has been stored less than 180 days only when authorized by a valid warrant.[124] If an electronic communication is stored longer than 180 days, authorities may obtain access to it through an administrative, grand jury, or trial subpoena, or through a court order supported by a reasonable belief that the contents of the communication are relevant to a law enforcement

---

119. 18 U.S.C. § 2707(b)(1). Evidence will also be suppressed if a Fourth Amendment violation can be demonstrated.

120. 18 U.S.C. § 2701(a).

121. The definition of electronic communications "service" complements the definition of "systems," extending protection to any service that provides users with the ability to send or receive electronic communications. 18 U.S.C. §2703(a). "'Remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

122. *See* 18 U.S.C. § 2510(14).

123. *See supra* text accompanying notes 82-89.

124. As previously discussed, the ECPA includes an emergency provision for warrantless searches if the government determines that disclosure to the user may result in the destruction of the information sought. *See* 18 U.S.C. § 2704(a)(5); *supra* text accompanying notes 97-99. This determination is not appealable by either the user or the service. *See* 18 U.S.C. § 2704(a)(5).

inquiry. Subpoenas and other court orders can only be executed after giving notice to the user, although a valid warrant can be executed without providing notice.[125]

Another vital provision of Title II allows a computer system's owner to challenge the scope of the search. If a court order or warrant authorizes a search or seizure of stored electronic communications, the provider of the computing services may request that the court modify or quash the order.[126] To have the order modified or quashed, the provider of the computing service must show that the information or records requested are "unusually voluminous in nature" or that compliance with the order "would cause an undue burden" on the service provider.[127]

Title II also prohibits the nonconsensual disclosure to government entities of information other than the contents of communications to the government,[128] unless compelled by subpoena, warrant, or court order.[129] This provision protects information such as the identities of the recipient and sender of a stored electronic mail message, the length of a message, the types of services that a user utilizes, and where a user is physically located. However, an electronic communication service may disclose this type of information about a system user to a private party.[130]

In this respect, electronic communications enjoy more protection after they are stored than during their transmission.[131] While Title II prohibits electronic communication services from disclosing information other than the contents of stored communications to law enforcement officers, Title I permits government authorities to determine the identity of the parties to an electronic communication and other information aside from the contents of the communication, if the communication is intercepted en route.[132]

The ECPA permits routine monitoring and maintenance by system operators. If system operators inadvertently discover incriminating information that affects users of the system, the system operator may take

---

125. *See* 18 U.S.C. § 2703(b).
126. *See* 18 U.S.C. § 2703(d).
127. *See id.*
128. *See* 18 U.S.C. § 2703(a).
129. *See* 18 U.S.C. § 2703(c)(1)(A).
130. *See id.*
131. This contrasts with laws related to telephone calls, which allow government entities to request stored information about telephone users and telephone calls (such as the numbers dialed by a party, the numbers that a party uses, and the duration of a call) provided the contents of a conversation are not divulged.
132. *See supra* note 106 and accompanying text.

appropriate disciplinary action.[133] However, the system operator may not divulge the contents of the communications to anyone.[134] Thus, an employer may fire an individual based on the contents of the employee's electronic mail messages stored on the company system, but the employer could not then divulge the contents of those communications to law enforcement personnel or other outsiders.

If inadvertent interception results in discovery of communications pertaining to the commission of a crime, disclosure is permitted.[135] However, the legislative history states that such evidence must relate to an "ongoing" criminal activity.[136] If courts accept this legislative history, an employer who inadvertently discovers evidence of a completed criminal activity will not be authorized to turn the evidence over to law enforcement officers.

A system user who is harmed by the system operator's disclosure of stored information can maintain a cause of action against the system operator. However, a system operator is only liable if he knowingly divulges the contents of communications to others.[137] If an operator operates the system recklessly or negligently, enabling outsiders to access the system, the aggrieved party would only have a cause of action against the outsiders.

If a system user believes that another user is snooping into her private stored communications, Title II permits the aggrieved user to raise a civil claim against the violator, even if the violator is another authorized user. The statute recognizes that a "public" system may have "private" zones, and that users of public systems may still have private files.[138] Authorized users of a system violate the ECPA by exceeding their authority and entering the private zones of a computer system.[139]

---

133. *See* 18 U.S.C. § 2701(c)(1).
134. *See* 18 U.S.C. § 2702(a)(1).
135. *See* 18 U.S.C. § 2702(b)(6).
136. ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3592.
137. 18 U.S.C. § 2702(a)(1).
138. 18 U.S.C. § 2701(a)(2); ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3589-90.
139. 18 U.S.C. § 2701(a)(2); ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3589-90.

2. Privacy Protection Act of 1980 ("PPA")

The Privacy Protection Act provides that:

> Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation . . . of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast or other similar form of public communication.[140]

Congress enacted the Privacy Protection Act ("PPA") in order to lessen the chilling effect of intrusive searches on those engaged in First Amendment activities.[141] The PPA prevents government officials from using search warrants and other unannounced searches to probe the work product and other documentary materials of the press and others who disseminate public communications. Instead, law enforcement officers must use subpoenas or voluntary cooperation when seeking evidence from those engaged in First Amendment activities.

The PPA does not immunize the press from searches. But by requiring that searches be conducted via subpoena rather than by search warrant, the Act mandates that searches be conducted through a relatively unintrusive method.

Many types of computer systems appear to fall within the forms of public communication protected by the Act. Obviously, the computer systems of traditional media entities such as newspapers, magazines and broadcasters would be protected from unannounced searches by law enforcement officers. Courts have not yet addressed the status of BBSs or on-line databases under the PPA. The only court to face a PPA challenge to the search of a BBS specifically avoided resolving the question of whether the BBS was protected by the PPA.[142] If courts consider BBSs or

---

140. 42 U.S.C. § 2000aa(a) (1988).

141. *See* S. REP. NO. 874, 96th Cong., 2d Sess. 4-8 (1980), *reprinted in* 1980 U.S.C.C.A.N. 3950, 3950-54 [hereinafter PPA Legis. Hist.].

142. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 434 n.1 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994). The *Steve Jackson Games* court held that the computers of the plaintiff corporation fell within the protection of the PPA since the corporation published books, magazines, board games and related products. The court therefore did not have to resolve, and in fact avoided resolving, the question of whether the

on-line databases to be "broadcasters" or "disseminators of public communication" within the meaning of the PPA, nonconsensual searches of these computer systems by law enforcement officials could only be conducted through a subpoena or with the consent of the system operator.

Most types of BBSs certainly appear to fall within the statutory definition of newspaper, broadcaster, or other similar form of public communication. Like newspapers and broadcasters, BBSs are a form of communication that disseminate their content to thousands, and potentially millions, of subscribers. These subscribers rely on the system to provide them with information, discourse, and differing points of view on an incredibly diverse range of topics. Individual BBSs such as CompuServe, America On-Line, and The Well contain conferences on a wide range of political, work-related, leisure, or lifestyle topics. And unlike newspapers or television or radio broadcasters, a BBS permits the subscribers to control the content of the messages transmitted. For the first time, an individual user can disseminate their point of view to a large number of geographically separated people without having the message filtered by the editorial process of a newspaper or broadcaster. To deprive this type of system of the protections of the PPA would distort the plain meaning of "public communication."[143] Protecting BBSs under the PPA would be consistent with congressional intent, since its legislative history provides explicitly that Congress intended that "form of public communication" have "a broad meaning."[144]

If BBSs and on-line systems are protected under the PPA, their hardware is protected. The PPA protects work product materials and other documentary materials.[145] As discussed in part III.C of this article, the physical hardware of a BBS falls within the PPA's definition of documentary materials, especially since BBS postings generally exhibit the creative mental process necessary to qualify as "work product" under the PPA.

The PPA only appears to protect the physical hardware of a system, and does not appear to protect information that lacks a material physical manifestation. The PPA protects "documentary materials," defined as

---

BBS, standing alone, would have fallen within the PPA.

143. *See infra* part III.C.

144. PPA Legis. Hist., *supra* note 141, 1980 U.S.C.C.A.N. at 3957.

145. *See* 42 U.S.C. § 2000aa. Consistent with the PPA, the U.S. Department of Justice has adopted regulations governing searches of those engaged in First Amendment activities. These "Guidelines on Methods of Obtaining Documentary Materials Held by Third Parties" explicitly applies to "materials upon which information is electronically or magnetically recorded." 28 C.F.R. § 59.2(c) (1994).

"materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, . . . and other mechanically, magnetically or electronically recorded cards, tapes and discs."[146] While this extends to all current forms of computer memory, it does not extend to mere information downloaded onto hardware owned by law enforcement officials. However, such protection is unnecessary for BBSs, since the ECPA and the Fourth Amendment provide adequate protection for private computer communications that lack a tangible manifestation.[147]

The PPA and Justice Department guidelines promulgated under it[148] permit searches if conducted on those actually suspected of participation in the criminal activity under investigation.[149] However, Congress did not intend the "suspect exception" to apply when the only offense the possessor is suspected of committing is the receipt, possession, communication or withholding of the very materials sought by law enforcement officials.[150]

It is important to note that a violation of the PPA will *not* lead to the suppression of evidence.[151] Civil actions against government entities, agencies, or individual agents for "actual damages but not less than liquidated damages of $1,000" are the exclusive remedy for violations of the PPA.[152]

C. State Constitutional and Statutory Protection

The Fourth Amendment provides a minimum standard governing searches and seizures by state law enforcement authorities.[153] However, many states impose constitutional or statutory standards exceeding those established by the Federal Constitution. Almost all state constitutions contain a provision protecting an individual's right to be free from unwanted searches and seizures. Ten state constitutions go beyond this and contain provisions explicitly protecting an individual's right of

146. 42 U.S.C. § 2000aa-7(a).
147. *See infra* parts III.A-B.
148. 28 C.F.R. § 59.2(c) (1994).
149. *See* United States v. Mittelman, 999 F.2d 440, 443 (9th Cir. 1993).
150. PPA Legis. Hist., *supra* note 141, 1980 U.S.C.C.A.N. at 3957.
151. 42 U.S.C. § 2000aa-6(e).
152. 42 U.S.C. § 2000aa-6(a), (d), (f).
153. *See* Mapp v. Ohio, 367 U.S. 643, 647-49 (1967) (holding that the Fourteenth Amendment guarantee of due process incorporates the Fourth Amendment).

privacy.[154] Many state courts have adopted precedents granting individuals rights broader than those recognized under federal precedents,[155] since "individual states may surely construe their own constitutions as imposing more stringent constraints on police conduct than does the Federal Constitution."[156] A complete examination of these local standards is beyond the scope of this article.[157] However, practitioners should remain aware of the possibility that local precedents may provide a more expansive right to be free from unwanted searches and seizures than those provided by the Fourth Amendment, the ECPA, or the PPA.

II. STAND-ALONE COMPUTERS AND STORAGE MEDIA

For stand-alone computer systems and their storage media, the scope of searches and the return of the hardware to the owner present the most important unresolved search and seizure questions. As discussed previously, the ECPA does not apply to stand-alone systems, and the PPA

---

154. ALASKA CONST. art. I, § 22; ARIZ. CONST. art. II, § 8.; CAL. CONST. art. I, § 1; FLA. CONST. art. I, §§ 12, 23; HAW. CONST. art. I, §§ 6, 7; ILL. CONST. art. I, §§ 6, 12; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7. For example, the California Supreme Court stated: "Common experience with the ever-increasing use of computers in contemporary society confirms that the [state constitutional privacy provision was] needed and intended to safeguard individual privacy from intrusion by both private and government action." Hill v. NCAA, 865 P.2d 633, 643 (Cal. 1994) (in bank).

155. *See* State v. Gunwall, 720 P.2d 808, 814 (Wash. 1986) (en banc) (rejecting Smith v. Maryland, 442 U.S. 735 (1979), in holding that police monitoring of telephone numbers dialed by an individual violated the state constitution); People v. Sporleder, 666 P.2d 135 (Colo. 1985) (same); State v. Tanaka, 701 P.2d 1274 (Haw. 1985) (holding that Hawaii recognizes that individuals have an expectation of privacy in their garbage, contrary to near-unanimous holdings of federal courts of appeals); State v. Owen, 453 So. 2d 1202, 1205 (La. 1984) (holding that any individual adversely affected by a search or seizure may challenge the search or seizure); People v. Brisendine, 531 P.2d 1099, 1109 (Cal. 1979) (holding that the permissible scope of search incident to arrest is narrower than that recognized in United States Supreme Court decisions); State v. Glass, 583 P.2d 872 (Alaska 1978) (rejecting United States v. White, 401 U.S. 745 (1971)); State v. Saunders, 381 A.2d 333 (N.J. 1976) (invalidating state fornication law). *See generally* Mark Silverstein, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 ILL. L. REV. 215 (1989).

156. California v. Greenwood, 486 U.S. 35, 43 (1988).

157. The LaFave treatise contains comprehensive citations to several dozen law review articles that discuss this point in more depth, and also includes citations to numerous state court decisions in which an individual's right to be free from unwanted searches and seizures exceeds that protected by the Fourth Amendment. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 1.5 (2d ed. 1987 & 1994 Supp.). Another excellent source is *Special Project: The Continuing Evolution of Criminal Constitutional Law in State Courts*, 47 VAND. L. REV. 795 (1994).

protects only stand-alone systems that law enforcement personnel would have reason to believe contain work product materials of those who disseminate public communications. As a result, the Fourth Amendment serves as the primary source of protection for stand-alone computer systems.

A. The Appropriate Expectation of Privacy

Individuals should have little difficulty establishing a high expectation of privacy in their computers, especially when those computers are located in their homes.[158] Home computers are exactly the sort of repositories of personal information that the Fourth Amendment protects most heavily.

Although individuals should have little difficulty establishing an expectation of privacy in their own computers, an individual will have more difficulty establishing an expectation of privacy in data stored on a stand-alone computer owned by a third party. Fourth Amendment rights are personal. A defendant cannot claim a violation based on a search of a third person's property.[159] One only has an expectation of privacy in property when they can show ownership, lawful possession or lawful control of the place searched.[160] The only federal court directly to address this issue found that the defendant lacked standing to challenge a search of her co-defendant's home computer, since she failed to show any ownership or possessory interest in the records stored in the computer.[161] Unless an individual owns a computer located in another's home, or has exclusive control over files or programs stored on another person's computer, courts will likely decline to find an expectation of privacy in the stored information.

B. Particularity of Warrants and the Scope of a Search or Seizure

1. The Intermingled Documents Problem

Law enforcement efforts to seek evidence stored on computers raise

158. *See supra* text accompanying notes 31-32.
159. *See* Rakas v. Illinois, 439 U.S. 128, 133-34 (1978).
160. *See id.* at 143 n.12.
161. United States v. Taylor, 92-CR-322 (CSH), 1992 WL 249969, at *19 (S.D.N.Y. Sept. 22, 1992).

serious questions regarding overbroad searches and seizures. Searches and seizures of computer storage media will force courts to resolve an unsettled and long-standing Fourth Amendment problem: how to resolve situations in which relevant documents subject to lawful search or seizure are intermingled with highly personal documents not otherwise subject to search or seizure. This intermingled documents problem has not received a great deal of attention in the case law, and remains a relatively undeveloped area of Fourth Amendment law. However, the two circuit courts to address the issue directly have formulated a special doctrine to handle these searches.[162] The leading commentators on search and seizure law have endorsed this doctrine, and other cases endorse it or cite it with approval.[163] The doctrine strikes a sound balance between the privacy interests protected by the Fourth Amendment and the need for law enforcement officers to conduct effective searches and seizures, and should be adopted for searches of high-volume computer storage media such as hard disks.

In 1976, the Supreme Court expressed particular concern over the risks posed by overbroad and insufficiently particular searches when the government seeks information instead of contraband or the physical evidence of a crime:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in

---

162. *See* United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982); United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987).

163. *See* LAFAVE, *supra* note 157, § 2.6(e); MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE § 220.5 (ALI 1975); *see also* United States v. Abram, 830 F. Supp. 551, 554 (D. Kan. 1993) (citing *Tamura*, and holding that wholesale seizure of intermingled documents for later examination without intervening magistrate supervision violated the Fourth Amendment); United States v. First Nat'l City Bank, 568 F.2d 853, 861 (2d Cir. 1977) (Gurfein, J., concurring and dissenting) (criticizing dicta in majority opinion, and endorsing the ALI/*Tamura* approach for an IRS search of the contents of a safe deposit box); Nixon v. Adm'r of Gen. Servs., 408 F. Supp. 321, 363 n.57 (1976), *aff'd*, 433 U.S. 425 (1977) (citing ALI intermingled documents approach with approval, and noting that this approach was essentially followed by rules promulgated under the Presidential Recordings and Materials Preservation Act for separating public presidential documents from private presidential documents).

> fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a warrant for the "seizure" of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.[164]

Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information. However, this very quantity and variety of information increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized.

"[T]he seizure of one thing under a warrant describing another"[165] and a general rummaging around for information[166] are the specific harms that the overbreadth doctrine addresses. Since it is not possible to physically separate information stored on a computer disk, searches of computers will almost inevitably involve the seizure of irrelevant information along with the relevant information. Relevant files can only be sifted from irrelevant files by examining the stored computer data.

The rule controlling searches of intermingled documents originated by the Ninth Circuit in *Tamura*, and endorsed by the Fourth Circuit in *Shilling*, should be applied to computer storage media. This rule holds that where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents.[167] If the officers know prior to the search that transporting large quantities[168] of documents or hardware is likely, they can apply to the

---

164. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

165. *Id.* at 480 (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).

166. United States v. Thomas, 746 F. Supp. 65, 67-68. (D. Utah 1990); *see* Chimel v. California, 395 U.S. 752, 767 (1969) (condemning rummaging "at will" through private papers "in search of whatever will convict").

167. *See* United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982); United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987).

168. The cases upholding the seizure of intermingled documents have involved small numbers of documents. *See* United States v. Slocum, 708 F.2d 587, 605-06 (11th Cir. 1983) (seizure of only one file folder); United States v. Beusch, 596 F.2d 871, 876-77 (9th Cir. 1979) ("[W]e are careful to point out that we are discussing single files and single ledgers. . . . The reasons we have given for allowing their seizure may not apply to sets of ledgers or files.").

magistrate issuing the warrant for permission to remove such material; permission should be granted only when on-site sorting of relevant and irrelevant material is infeasible and no other practical alternative exists.[169] "The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."[170]

The leading treatise on search and seizure law and the American Law Institute's *Model Code of Pre-Arraignment Procedure* both endorse this rule.[171] As one court has noted: "The wholesale seizure for later detailed examination of records not described in a warrant is the kind of investigatory dragnet that the fourth amendment was designed to prevent."[172]

The *Tamura* rule effectively balances the privacy needs of the individual against the need for law enforcement officers to conduct searches in the course of investigating possible criminal activity. By permitting the removal of computer hardware, the *Tamura* rule anticipates the exigent circumstance that to prevent the destruction of evidence, the computer disks may need to be removed from the premises for further analysis. Practical considerations and the fear of destruction or alteration of evidence mandate that officers remove computer memory from the suspect's control when a large quantity of information is discovered.[173]

---

169. *See Tamura*, 694 F.2d at 595-96.

170. *Id.* at 596.

171. *See supra* note 163.

172. United States v. Abram, 830 F. Supp. 551, 554-55 (D. Kan. 1993) (quoting *Tamura*, 694 F.2d at 595); *see also* United States v. Robbins, 21 F.3d 297, 300 (8th Cir. 1994) (citing *Tamura*, 694 F.2d at 595 n.2, and holding that officers could not seize a wallet and search, at a later time, items intermingled in the wallet merely because the warrant permitted a search for cash receipts); People v. Economy, 631 N.E.2d 827, 833 (Ill. App. 1994) (finding no Fourth Amendment violation where police seized file cabinets in a search for drugs, since police did not look through documents contained in files).

173. Several cases have upheld the *seizure* of irrelevant documents intermingled with documents within the scope of a warrant. However, these cases have been careful not to endorse wholesale *searches* of documents beyond the scope of the warrant, aside from brief examinations of the documents to determine whether they fall within the scope of the warrant. *See* United States v. Christine, 687 F.2d 749, 760 (3d Cir. 1982) (noting that "in searches for papers, it is certain that some innocuous documents will be at least cursorily perused in order to determine whether they are among those papers to be seized"); United States v. Wuagneux, 683 F.2d 1343, 1352 (11th Cir. 1982), *cert. denied*, 464 U.S. 814 (1983) (holding that agents may lawfully review documents on site to determine whether they fall within the warrant, and when necessary seize entire files so that agents can identify where individual documents belong if returned); United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981) (Documents may be reviewed briefly to determine whether probable cause exists for their seizure. If their incriminating character is obvious, the documents may be seized; otherwise, the review must cease when the warrant's inapplicability to a particular document becomes clear); United States v. Slocum, 708 F.2d 587, 605-06 (11th Cir. 1983) (approving the seizure of an entire file after on-site review determined that it contained documents within the scope of the warrant, since seizing the whole file helped limit the time

Once computer data is removed from the suspect's control, there is no exigent circumstance or practical reason to permit officers to rummage through all of the stored data regardless of its relevance or its relation to the information specified in the warrant. After law enforcement personnel obtain exclusive control over computer data, requiring them to specify exactly what type of files will be inspected does not present any undue burden. A neutral magistrate should determine the conditions and limitations for inspecting large quantities of computer data. A second warrant should be obtained when massive quantities of information are seized, in order to prevent a general rummaging and ensure that the search will extend to only relevant documents.

The *Tamura* rule is well suited to the practical considerations involved in searching through computer memory. Once officers seize large quantities of computer memory, they have three methods of distinguishing relevant from irrelevant information. Officers can either read through portions of each file stored in the memory, conduct a key word search of the data stored on the disks, or print out a directory of the title and file type for each file on the disk.[174]

The effectiveness of key word searches to investigators and their importance in protecting privacy were recognized by both the Fifth Circuit and by the United States Secret Service in *Steve Jackson Games*. In that case, the court noted that key word searches could limit intrusions into personal privacy since: "[A]s the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications. For example, the Secret Service claimed . . . that it reviewed the private E-mail on the BBS by use of key word searches."[175]

Law enforcement officers, particularly federal officers, are sufficiently familiar with computer searches, and the likelihood that large quantities of personal information will be intermingled with relevant information, to be required to apply beforehand for permission to perform a large scale-removal of computer storage media.[176] A magistrate's review of the

---

necessary to conduct the search); United States v. Goff, 677 F. Supp. 1526, 1544 (D. Utah 1987) (holding that officers may conduct a brief review of computer disks at site of search to determine their relevancy).

174. *See In re* Subpoena Duces Tecum, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (noting that "it is easier in computer age to separate relevant from irrelevant documents").

175. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994).

176. *See, e.g.*, Klitzman, Klitzman, and Gallagher v. Krut, 744 F.2d 955, 961 (3d Cir.

methods used to separate relevant from irrelevant information is necessary to ensure that the officers only read through files that there is reason to believe contain relevant information.

Once law enforcement officials seize a computer storage device, these officers should be required to specify which types of files are sought. Whenever possible, key word searches should be used to distinguish files that fall within the scope of a warrant from files that fall outside the scope of the warrant. In addition, the type of information stored in a particular file is often easily ascertainable. Computer programs store information in a wide variety of formats. For example, most financial spreadsheets store information in a completely different format than do word processing programs. Similarly, an investigator reasonably familiar with computers should be able to distinguish database programs, electronic mail files, telephone lists and stored visual or audio files from each other. Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought. Where relying on the type of computer files fails to narrow the scope of the search sufficiently, the magistrate should review the search methods proposed by the investigating officers. Opposing counsel should be given the opportunity to propose less intrusive methods of screening the information. Alternatively, opposing counsel should be given an initial opportunity to identify those files that it believes fall outside the scope of the search. If the investigating officers are unable to provide any reason to believe that those files fall within the scope of the search, or are unable to propose any method for determining the relevance of these files, a search of these files should not be permitted. The basic principle is that before a wide-ranging exploratory search is conducted, the magistrate should require the investigators to provide an outline of the methods that they will use to sort through the information.

Of course, the facts of some cases, such as complex conspiracies, may justify the full-text search of all or mostly all of the records. However, the government should bear a heavy burden in demonstrating that no less intrusive method is available to separate files falling within the scope of the warrant from files falling outside the scope of the warrant. A vague

---

1984) (noting that federal officers should have been aware of, and followed, U.S. Attorney Guidelines of C.F.R. § 59.1-6 (1994), which the government must meet before using a search warrant to obtain documentary materials held by disinterested third parties).

allegation that the nature of computer storage somehow requires a full text review of all files in all situations should not be permitted to eviscerate the Fourth Amendment's particularity requirement. A warrant providing for the search and seizure of information pertaining to certain enumerated transactions or events stored on "computer storage disks and related equipment" provides no more justification for the subsequent search of *all* files discovered on those disks than would a warrant providing for the search of "papers and other written records" permit the seizure of *all* documents and records discovered on the site.

2. *The Intermingled Documents Approach Compared to the Closed Container Approach*

A recent case in the Southern District of New York appears to follow the logic of the *Tamura* approach.[177] The district court quashed a grand jury subpoena for a corporation's hard disks, finding the subpoena unreasonably broad. The court reasoned that relevant information was too intermingled with irrelevant information to permit a wholesale search of the entire contents of the disks. The court recognized that the government had the ability to separate relevant information from irrelevant information by means of key word searches, and thus did not need to search through the entire contents of the hard disks.[178]

But aside from the *In re Subpoena Duces Tecum* case, courts have not recognized that searches of computer memory present any special overbreadth problems. In two other cases, federal courts upheld searches and seizures of large quantities of computer data,[179] and three other cases upheld searches of the extremely small computer memory capacity of telephone pagers[180] without requiring any preliminary determination of the relevancy of the data. These cases all relied on an analogy between

---

177. *In re Subpoena Duces Tecum*, 846 F. Supp at 13.

178. *Id.* at 12-13; *see Collecting Evidence in the Age of E-Mail*, AM. LAWYER, July/Aug. 1994, at 119 (discussing various methods of searching computer files, and emphasizing that key word searches are the most thorough, effective, and efficient method of searching large quantities of computer data).

179. United States v. Hersch, CR-A-93-10339-2, 1994 WL 568728 (D. Mass. Sept. 27, 1994); United States v. Sissler, No. 90-CR-12, 1991 WL 239000 (W.D. Mich. Aug. 30, 1991), *aff'd*, 966 F.2d 1455 (table), 1992 WL 126974 (6th Cir. 1992) (unpublished disposition), *cert. denied*, 113 S. Ct. 1004 (1993).

180. United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993); United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991); United States v. Blas, No. 90-CR-162, 1990 WL 265179 (E.D. Wis. Dec. 4, 1990); *supra* notes 34-35 and accompanying text.

computer storage media and closed containers in order to find support in existing Fourth Amendment case law.

In order to convince courts to accept the *Tamura* approach, computer owners must demonstrate that reliance on the container analogy is ill-advised in computer cases. An analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage.

The closed container rule originated in cases involving searches for weapons, contraband, and other physical instrumentalities or fruits of a crime.[181] However, as the Supreme Court has noted, "there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable."[182] A container can be inspected relatively rapidly to determine whether contraband, such as narcotics or weapons, is present. However, the relevance of information stored on a computer disk can only be determined by reading the information stored on the disk. Reading through the enormous quantity and variety of information stored on a computer disk presents a much greater intrusion into an individual's privacy than would a short examination of a handbag or suitcase.

The container rule, if applied to computer storage, effectively permits an "all records" search. When officers seek information or documents, a sufficiently particular warrant must describe the *subject matter* of the information sought, not merely the form in which the information is stored.[183] If courts would invalidate a warrant providing for the search of "all documents stored on paper," there is no reason that a court should uphold a warrant providing for the search of "all information stored on computer or magnetic storage media."

Application of the container rule to computer memory devices essentially permits law enforcement officers to rummage through any and

---

181. *Compare* Illinois v. Andreas, 463 U.S. 765, 771-72 (1983) (finding no expectation of privacy in drugs discovered in a container after the container was opened, since the contraband nature of drugs immediately gave officers probable cause to believe it was connected with illegal activity) *with* United States v. Knoll, 16 F.3d 1313 (2d Cir. 1994) (holding that if files within a closed container remain closed, and if their relevancy is not apparent from the exterior, the owner maintains an expectation of privacy in the files entirely separate from the expectation of privacy in the container).

182. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

183. United States v. Thomas, 746 F. Supp. 65, 68 (D. Utah 1990) (discussing a search that included computer disks in a corporate office, and holding that a warrant must limit the search to a "particular entity or transaction" in order to be reasonably particular).

all information stored on a computer disk whenever the officers obtain possession of the physical computer hardware. However, Fourth Amendment law has long since abandoned the concept that physical possession of property by law enforcement officers makes any subsequent search constitutional.[184] Discussing warrantless searches, the Court stated: "The scope of a warrantless search . . . is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found."[185] And in the context of computer searches, courts agree that an individual has a separate expectation of privacy in the *contents* of computer memory than the individual has in the hardware the information is stored on.[186]

Instead of trying to solve this complex issue by simply categorizing computer memory as a "container," courts must formulate a rule that recognizes both the needs of law enforcement personnel and the privacy interests of computer users. One court has acknowledged that the intangible nature of stored computer memory makes analogies to searches of traditional physical objects, such as books, inappropriate.[187] Application of the container rule to computer storage media ignores the reality of modern computer use and allows officers to gain a window into all aspects of a suspect's life merely because the officers suspect that one piece of relevant information may be stored on a computer. *Tamura*'s intermingled documents doctrine, in contrast, effectively balances the needs of law enforcement officers against the Fourth Amendment rights of suspects. Under *Tamura*, law enforcement officers will still have the ability to look through computer files that there is some reason to believe contain relevant information, and to execute key word searches to examine all files stored in a computer. However, the doctrine protects an individual's expectation of privacy in other information stored on the computer.

---

184. "'The premise that property interests control the right of the government to search and seize has been discredited.'" United States v. Katz, 389 U.S. 347, 362 (1967) (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).

185. United States v. Ross, 456 U.S. 798, 824 (1982).

186. United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); United States v. Blas, No. 90-CR-162, 1990 WL 265179, at *20 (E.D. Wis. Dec. 4, 1990).

187. *Blas*, 1990 WL 265179, at *20.

C. Encrypted Data

The *Tamura* rule will not prevent officers from defeating passwords, encryption mechanisms, or other security measures applied to computer data. A lawful seizure of evidence carries with it the right to use available scientific methods to examine and enhance the evidence.[188] For example, in *Commonwealth v. Copenhefer*,[189] law enforcement officers obtained a warrant for the computer of a suspect in a kidnapping and murder investigation. By the time the officers seized the computer, the suspect had already deleted incriminating evidence previously stored on it. The law enforcement officers used software to recover the deleted files, which formed an important part of the prosecution's case. The court held that a separate warrant was not required to search the hard disk for the deleted files.[190]

D. Return of Equipment

Deprivation of computer hardware, software, or data can cause severe hardships to individuals or corporations. These hardships are exacerbated when the computer equipment is seized without notice to the computer user or without an opportunity to make back-up copies of important files. As computer BBSs have discovered, government efforts to search or seize the files of a single user of a multi-user computer system can deprive the system owner of the use of his or her equipment, causing tens of thousands of dollars of lost revenue and threatening smaller systems with bankruptcy.[191]

When the government lawfully seizes computer equipment, it must

---

188. LAFAVE, *supra* note 157, § 4.10(e). *See* Commonwealth v. Copenhefer, 587 A.2d 1353 (Pa. 1991); State v. Warren, 306 S.E.2d 446, 449 (N.C. 1983) (holding that bloodstains seized under a valid warrant could be subjected to chemical tests without a separate warrant); State v. Petrone, 468 N.W.2d 676, 681 (Wis. 1991) (finding the developing of photographic film to be within the scope of the warrant); People v. Scheidt, 492 N.E.2d 248, 251 (Ill. App. 1986) (holding that the police were authorized to decipher symbols and abbreviations on horse betting slips); *but see* Thomas Krivulka, Note, *Limits of Privacy Expectations Within Seized Electronic Data*, 65 TEMP. L. REV. 645 (1992) (criticizing *Copenhefer* as wrongly decided).

189. 587 A.2d 1353 (Pa. 1991).

190. *Id.* at 1356; *see also Securing Your Data*, A.B.A. J., June 1994, at 58 (discussing a Canadian civil case in which the defendant deleted incriminating information from the disks before producing them in discovery, leading the court to permit the plaintiff to recover the deleted files).

191. *See supra* note 11 (citing relevant cases).

generally return the equipment to the owner when it has finished examining the equipment for evidence of a crime.[192] The government may retain seized software or hardware only if the equipment is forfeitable, which generally requires that the equipment contain evidence of criminal activity.[193] If the government gives away, loses, or destroys seized property, the aggrieved party may seek damages.[194]

Fed. R. Crim. P. 41(e) provides: "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." If the court orders the return of the property, the court may impose reasonable conditions to preserve access in future proceedings.[195] The district court retains equitable jurisdiction to award damages if the government gives away, loses, or destroys a person's property seized in a search, even if the search was lawfully conducted.[196]

A suspect can petition for the return of seized equipment either before or after an indictment is issued.[197] Since return of the seized equipment is an equitable remedy, suspects must show irreparable harm and the absence of an adequate remedy at law in order to prevail;[198] some courts require an additional showing that the government seized the items through callous disregard of the Fourth Amendment and that the movant had an interest in the property.[199]

---

192. FED. R. CRIM. P. 41(d) (when officers seize material under a warrant "return shall be made promptly and shall be accompanied by a written inventory of any property taken"); *see* Soviero v. United States, 967 F.2d 791, 792-94 (2d Cir. 1992) (holding that a convicted defendant was entitled to seek damages for value of software destroyed by the government and to obtain the return of seized computer hardware).

193. *See Soviero*, 967 F.2d at 793.

194. *Id.*; Mora v. United States, 955 F.2d 156, 159 (2d Cir. 1992).

195. *See* Ramsdan v. United States, 2 F.3d 322, 324-25 (9th Cir. 1993) (allowing the state to review or copy records even though the original versions were returned to their owner), *cert. denied*, 114 S. Ct. 1624 (1994).

196. *Mora*, 955 F.2d at 159-60.

197. *Ramsdan*, 2 F.3d at 324-25 (holding that suspect can seek return of seized materials prior to indictment under court's equitable jurisdiction, or after indictment under Fed. R. Crim. P. 41(e)).

198. *See* Industrias Cardoen, Ltda. v. United States, 983 F.2d 49, 51 (5th Cir. 1993) (finding that actions seeking the return of property are governed by equitable principles whether based on Fed. R. Crim. P. 41(e) or on the general equitable jurisdiction of the federal court); Kitty's East v. United States, 905 F.2d 1367, 1370-71 (10th Cir. 1990).

199. *Ramsdan*, 2 F.3d at 324-25 (noting that movant must establish callous disregard of the Fourth Amendment, an individual interest in the property, irreparable injury if relief is not granted, and absence of an adequate remedy at law). *See also* Richey v. Smith, 515 F.2d 1239, 1243-44 (5th Cir. 1975); *but see* Kiesel Co. v. Householder, 879 F.2d 385, 387 (8th Cir. 1989) (holding that the movant is not required to show she possessed an interest in the property), *cert. denied*, 494 U.S. 1026 (1990).

When the government seizes a hard disk containing a wide variety of information, the disk owner should immediately have the government identify the specific files it seeks. Certain files are likely to contain information obviously unrelated to the information sought by the warrant and may be protectable from government examination.[200] Aggrieved parties must convince the court of the ease of copying computer storage media in order to persuade the court to grant an early return of the files. A bit-by-bit copy of even large capacity disks can be performed in a matter of minutes with the appropriate equipment. Given the fact that "deprivation of the property may be injurious even where the seizure is lawful,"[201] aggrieved parties may be able to obtain equitable relief granting them the right to make a copy of the seized files, with the understanding that the government will retain the originals as part of an investigation.[202]

III. ON-LINE SYSTEMS AND ELECTRONIC BULLETIN BOARDS

The role of on-line computer systems and electronic bulletin boards[203] in public communication requires that monitoring, searching, and seizing these systems be subject to a different legal analysis than that applied to stand-alone computers and office networks. Unlike stand-alone systems and office networks, BBSs serve as a means of discourse and communication for the general public. Surveillance and seizure of public communications implicate the ECPA, the PPA, and the First Amendment, as well as the Fourth Amendment. The legality of a particular search, seizure or monitoring operation depends on a variety of factors, including the precise nature of the BBS system, the general public's ability to access the particular communications at issue, and the identity of the party intercepting the communications. Given the role of BBSs in public discourse, efforts to shut down these systems or seize their system hardware is

200. *See* United States v. Falon, 959 F.2d 1143, 1146-48 (1st Cir. 1992) (holding that in search of an individual's home, the broad categories of items that may be seized must be sufficiently linked to the alleged criminal activity so as to distinguish them from irrelevant material).

201. *In re* Southwestern Equip. Co. Search Warrant, 746 F. Supp. 1563, 1581 (S.D. Ga. 1990).

202. *See id.*

203. BBSs are distinct from on-line computer systems that support multiple users and time-sharing. However, both types of systems will be referred to as BBSs in this section.

subject to a special level of scrutiny.

A. Monitoring and Intercepting the Contents of BBS Communications

On-line communications services are a rapidly expanding business, generating over $500 million in annual revenue.[204] Users upload and download several million public and private messages over these systems each day. Large nationwide on-line services such as CompuServe and America On-Line join over 45,000 smaller BBSs to serve this growing market. Some are general interest systems containing information on a wide variety of topics. Others are narrowly targeted services, catering only to those with specific professional, personal, or political interests.

The increased popularity of BBSs has brought with it an increased surveillance of BBS communications by both government officials and private parties. The FBI, the Secret Service, and local law enforcement officers monitor electronic bulletin boards in order to discover criminal activities and develop evidence, particularly in cases of child pornography and computer software piracy.[205] Private corporations have begun to monitor BBSs, especially when seeking evidence regarding software piracy, or when investigating copyright infringement of proprietary audio and visual works that have been digitized and copied via BBSs.[206]

The monitoring and seizure of BBS communications by law enforcement agents implicate two conflicting policy interests. On the one hand, the monitoring or seizing of communications by the government stifles the exchange of ideas. As Justice Douglas stated: "Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances. Free discourse—a First Amendment value—may be frivolous or serious, humble or defiant, reactionary or revolutionary, profane or in good taste; but it is not free if there is surveillance. Free discourse liberates the spirit,

---

204. Michael Schrage, *Revolution of On-Line Services*, WASH. POST, July 15, 1994, at F2.

205. *See* Barbara Kantrowitz et al., *Child Abuse in Cyberspace: Police Target On-Line Pedophiles*, NEWSWEEK, Apr. 18, 1994, at 40; *2 Convicted in Computer Pornography Case*, N.Y. TIMES, July 29, 1994, at B7; Peter H. Lewis, *Student Accused of Running Network for Pirated Software*, N.Y. TIMES, Apr. 9, 1994, at A1.

206. *See* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (civil suit by Playboy against BBS for providing the means for users to digitize and copy copyrighted Playboy photographs); Frank Music Corp. v. CompuServe, Inc., No. 93 Civ. 815 (JFK) (S.D.N.Y. filed Nov. 29, 1993) (class action suit claiming that CompuServe BBS provides means for users to digitize and copy copyrighted musical performances); Barbara Kantrowitz et al., *My Info Is Not Your Info: Publishers and Government Call for Protection Against Online "Data Snatchers,"* NEWSWEEK, July 18, 1994 at 54.

though it may produce only froth."[207] On the other hand, statutory and constitutional authority recognizes that law enforcement officials should be able to monitor communications that are otherwise freely accessible to the general public.

The Fourth Amendment and the ECPA resolve this conflict in favor of law enforcement authorities, permitting them to monitor public communications. However, the ECPA and the Fourth Amendment distinguish public communications from private communications, and protect private communications from unauthorized interception.

Neither the Fourth Amendment nor the ECPA protects public BBS communications, since public communications do not enjoy any expectation of privacy.[208] Posting a message in the publicly accessible areas of a BBS can be viewed as either putting the message into "plain view," or as voluntarily disclosing the information to all other parties. One loses any expectation of privacy in an otherwise private item by placing the item into plain view.[209] As a result, outsiders such as law enforcement officials may monitor BBS communications if those communications are stored or transmitted in a manner that is accessible to the public. Similarly, voluntary disclosure of information to another permits the other party to relay that information to law enforcement personnel without offending the Fourth Amendment.[210] The ECPA codifies these principles, explicitly permitting the sender or intended recipients of an on-line communication to disclose the contents of the communication to third parties, including law enforcement officers.[211]

Conversely, messages transmitted over these systems in a manner that is not accessible to the general public retain their private nature and are protected from search or seizure by the Fourth Amendment and the ECPA.[212] As previously discussed,[213] private BBS communications fall

---

207. United States v. White, 401 U.S. 745, 762-63 (1971) (Douglas, J., dissenting).

208. *See supra* text accompanying notes 47-48, 109-111.

209. *See* Horton v. California, 496 U.S. 128, 133-34 (1990) (holding that if an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy).

210. *See* Hoffa v. United States, 385 U.S. 293 (1966); United States v. Seidlitz, 589 F.2d 152, 158 (4th Cir. 1978), *cert. denied*, 441 U.S. 992 (1979).

211. 18 U.S.C. § 2702(b).

212. "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." United States v. Katz, 389 U.S. 347, 351-52 (1967). Even without the explicit protections of the ECPA, the logic of Fourth Amendment case law protecting traditional mail should extend to electronic mail. *Cf.* United States v. Villarreal, 963 F.2d 770, 773-74 (5th Cir. 1992) (noting that both senders and

within the plain language of the ECPA, provided the BBS meets the ECPA's minimal interstate commerce requirement. Such communications may only be intercepted if law enforcement officers satisfy the strict requirements necessary to gain court approval.[214]

Under these principles, government agents may join a BBS and monitor the messages posted on the system. In doing so, the government need not disclose its presence. As long as a government agent has accessed the system through a valid means, he does not need to reveal his presence to other users, and does not need to reveal his affiliation with law enforcement to the system operator. Similarly, private parties may monitor public BBS communications in order to develop evidence of wrongdoing. Individuals voluntarily disclose information to others at their own risk.[215] A BBS user's lack of knowledge about the identity of the other authorized users of the system does not raise any constitutional concerns.

A recent case involving corporate snooping on a BBS demonstrates these principles. In *Sega Enterprises, Ltd. v. Maphia*, an authorized user of the "Maphia" bulletin board informed Sega, manufacturer of the popular "Genesis" videogame system, that copyrighted Sega videogames were being copied via the Maphia BBS.[216] A Sega employee logged onto the BBS using the informant's password and pseudonym with the permission of the informant. Using the informant's BBS account, the Sega employee monitored BBS communications that were accessible to all BBS users, and gathered substantial evidence that copying was occurring with the support and encouragement of the BBS operator. Based largely on this evidence, the district court issued an ex parte order authorizing the seizure of the system hardware and entered a temporary restraining order shutting down the system.[217]

---

addressees of mail can reasonably expect that the government will not open and read their mail). This principle should provide protection for electronic mail and other private communications transmitted over BBS systems that fail to satisfy the ECPA's interstate commerce requirement.

213. *See supra* text accompanying notes 88-91.

214. An application for a wiretap must demonstrate that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried." 18 U.S.C. § 2518(3)(c) (1988). *See* United States v. Fernandez, No. 92-CR563, 1993 WL 88197, at *3 (S.D.N.Y. Mar. 25, 1993) (holding that the government need only make a showing of the *difficulty* of other investigative techniques, and need not show that such techniques have been exhausted).

215. *See supra* text accompanying notes 49-53.

216. 30 U.S.P.Q.2d (BNA) 1921 (N.D. Cal. 1994).

217. *Id.* at 1928-29.

The court found that Sega's monitoring of the system did not violate the Fourth Amendment.[218] Since Sega was a private entity acting without the knowledge of the government, Sega's activities did not implicate the Fourth Amendment. Nor did the court find that Sega violated the ECPA. Even though the Maphia BBS only had 400 users, the court reasoned that the BBS was accessible to the public, and that the Sega employee was therefore not intruding into any "private" communications protected by the ECPA. The court also held that access to the system through the informant's account and pseudonym constituted authorized access under § 2701(c)(2) of the ECPA. The court specifically noted that an investigator operating under an alias need not reveal his true identity if doing so would defeat the purpose of the investigation.[219]

Different questions arise when a BBS operator discovers incriminating private information sent or stored on the BBS. For example, a BBS operator may inadvertently discover that BBS users are transmitting electronic mail messages that reveal their involvement in a criminal activity. Unless the BBS operator acts as a government agent, the Fourth Amendment is not violated.[220] Nor will the ECPA protect the information, since the ECPA explicitly permits the system operator to disclose incriminating information to law enforcement authorities when a BBS operator inadvertently discovers communications pertaining to the commission of a crime.[221]

The ECPA provision permitting a system operator to divulge the contents of communications pertaining to criminal activity contains two significant ambiguities. First, the legislative history of this provision states that the system operator may only divulge information pertaining to "ongoing" criminal activity.[222] Second, the ECPA does not define what is meant by "inadvertent" discovery. A BBS user who finds that the system operator has divulged incriminating messages under this provision may therefore seek to suppress the incriminating message by challenging that the material was not inadvertently discovered or that the information pertains only to a *completed* criminal activity.

A party who believes that the BBS operator did not discover the messages inadvertently will have to ascertain exactly what led to the

---

218. *Id.* at 1928.
219. *Id.*
220. *See supra* text accompanying notes 19-20.
221. 18 U.S.C. § 2702(b)(6).
222. ECPA Legis. Hist., *supra* note 78, 1986 U.S.C.C.A.N. at 3592.

discovery of the incriminating message. The ECPA explicitly prohibits a BBS operator from engaging in "service observing" or randomly monitoring messages, unless the monitoring is performed for mechanical reasons or as part of service quality control checks.[223] Examining the general operating procedures of the system will help determine whether the BBS was operating within its own guidelines when it discovered the messages. A party may also want to produce expert testimony from BBS service professionals to ascertain whether the BBS that disclosed the incriminating messages exceeded the measures necessary for quality control or mechanical maintenance. A party relying on the fact that the message did not pertain to an *ongoing* criminal activity must convince a court to follow congressional intent as expressed in the legislative history.

B. Disclosure of User and Membership Lists and Information Other Than the Contents of a Communication

Situations in which the government or private litigants seek information about system users other than the contents of their communications raise separate questions and implicate the First Amendment as well as the Fourth Amendment and the ECPA. One highly publicized example of an effort to discover such information was the R.J. Reynolds Tobacco Company's efforts to obtain the user list of an anti-tobacco BBS.[224] Similarly, the government might seek user lists of BBSs suspected of catering to pedophiles or carrying illegally copied software. The government or private litigants might also seek records pertaining to a particular BBS user and attempt to discover a list of system resources the user accessed, discussions involving the user, and the identity of other participants in these discussions.

When outsiders unconnected to the government seek information other than the contents of a communication, the ECPA permits the BBS to divulge such information to a private party. In contrast, the ECPA does not permit the BBS to divulge the same information to a government entity unless required to by a warrant, subpoena, or other court order.[225] Without a court order, a government entity is only entitled to receive information that is readily accessible to the general public. Thus, the ECPA leaves a BBS operator the discretion to determine whether a

223. 18 U.S.C. § 2702(b)(2) (referring to 18 U.S.C. § 2511(2)(a)(i)).
224. *See supra* note 6.
225. 18 U.S.C. § 2703(c)(1)(A), (B).

private party is entitled to information aside from the contents of a communication. It also prohibits the government from obtaining information other than the contents of a communication without a court order unless the information is available to the general public.

In resolving the issue of what information the government may lawfully acquire, courts should look to the particular nature of the BBS to determine what types of information are generally available to its users. BBSs vary widely on the issues of whether they permit users to determine the true identity of other users or to compile user lists, and whether they allow users to determine what resources another user is accessing or when another person has been logging onto the system. If such information is generally available to system users, there is no reason to prohibit the government from obtaining it.

The First Amendment right to freedom of association supplements the ECPA and Fourth Amendment provisions governing access to user lists of BBSs. In a series of cases involving attempts by several southern states to obtain membership lists of the NAACP, the Supreme Court severely limited the government's ability to seize membership lists of organizations engaged in advocacy and other First Amendment activities.[226] In order to obtain membership lists of groups that advance political, economic, religious, or cultural beliefs,[227] the state must "convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest."[228] If the government satisfies this threshold test, the request must be narrowly tailored so as not unnecessarily to impact protected rights of speech, press, or association; the request may be curtailed if there is a showing that a particularized harm such as harassment or reprisals may result from the disclosure of the associational relationships.[229]

A similar analysis applies to civil discovery requests for membership lists.[230] If a BBS is forced to disclose a membership list in civil discovery, it is entitled at a minimum to a very strict protective order prohibiting the

---

226. Those engaged in merely commercial activities do not enjoy these enhanced protections. Only groups engaged in the advocacy of ideas and opinions have a First Amendment right to maintain the privacy of their affiliation. *In re* A Witness Before the Special Grand Jury, 722 F.2d 349, 353 (7th Cir. 1983).

227. NAACP v. Alabama, 357 U.S. 449, 462 (1958).

228. Gibson v. Florida Legis. Investigation Comm., 372 U.S. 539, 546 (1963).

229. *In re* Grand Jury Proceedings, 776 F.2d 1099, 1102-03 (2d Cir. 1985).

230. *See* Marshall v. Bramer, 828 F.2d 355, 359-60 (6th Cir. 1987) (permitting discovery of membership list of subgroup within Ku Klux Klan).

public release of the contents of the list.[231]

C. *Search and Seizure of the Physical Hardware of a BBS*

The PPA appears to bar most seizures of the physical hardware of BBSs. As previously discussed, the PPA provides a special level of protection for the "work product" and "documentary materials" of those who "disseminate to the public a newspaper, book, broadcast or other similar form of public communication."[232] Law enforcement officers must use a subpoena, summons, or similarly unintrusive method of obtaining such materials.[233] Government attempts to deprive distributors of information of the physical means of disseminating their work violates both the letter and the spirit of the PPA, which exists to protect the freedom of the press and other public broadcasters.

The status of BBSs under the PPA turns on two unresolved questions. First, do BBSs fall within the PPA's definition of those who "disseminate to the public a newspaper, book, broadcast or other similar form of public communication"? If so, what aspects of a BBS constitute protected "work product" and "documentary materials"? The PPA has generated few published opinions, but the nature and role of BBSs strongly indicate that they should fall within the plain language of the Act.

BBSs serve as a means for groups and individuals to disseminate their views to a wide audience. Although BBSs have a hybrid quality and can perform "common carrier" functions similar to those of a telephone company or a post office, the primary function of most BBSs is analogous to that of a newspaper or a television broadcast. Individuals or organizations electronically post messages of interest on BBSs to be accessed and read by other BBS users. Like newspapers or magazines, BBSs are usually divided by subject matter into sections. An individual section, usually called a conference or topic, may cover current events, politics, sports, entertainment, matters of professional and personal interest,

---

231. *See In re* The Courier-Journal, 828 F.2d 361, 362-63 (6th Cir. 1987) (companion case to *Marshall v. Bramer* discussing strict protective order to prevent any public court documents from mentioning any information obtained from KKK membership list).

232. 42 U.S.C. § 2000aa(a) (1988).

233. The PPA requires that these steps be taken as a matter of statutory compulsion. Consistent with these statutory requirements, the United States Department of Justice has adopted guidelines mirroring the requirements of the PPA. *See* United States Dep't of Justice, Guidelines on Methods of Obtaining Documentary Materials Held by Third Parties, 28 C.F.R. § 59 (1994).

classified advertisements, or other specialized areas.

BBSs and newspapers also share the fact that they vary widely in the size and scope of their target audience. Some of the 45,000 BBSs currently operating in the United States are general interest systems that cover an extremely broad variety of topics. Others are narrowly targeted special interest boards that count their subscribers in the thousands or even in the hundreds.

The most significant difference between BBSs and traditional media such as newspapers and television broadcasters is that BBSs offer their subscribers an unprecedented ability to contribute to the information distributed over the system. Generally, no editorial board controls the viewpoints expressed. A user with something to add can usually immediately post her viewpoint, thus adding new facts and opinions to an existing discussion.

Given the role of BBSs in empowering millions of Americans to publicly disseminate their political, social, and personal views, BBSs certainly appear to fall within the scope of the PPA. By extending its protections to "other similar form[s] of public communication," the plain language of the PPA establishes that the Act is not limited to newspapers, television, and radio broadcasting services. The legislative history notes that Congress intended that the phrase "forms of public communication" be read broadly, and that the PPA not be restricted to the press.[234] The Act protects "all those who have a purpose to disseminate information to the public."[235] It would be quite an anomaly if a statute entitled "First Amendment Privacy Protection" and intended to apply to those who disseminate social, political, and personal views to the public failed to protect the most important modern medium by which an ordinary American can disseminate her views to a wide spectrum of other members of the community.

Assuming that BBSs fall within scope of the PPA, the next question concerns what aspects of a BBS fall within the PPA's definition of "work product" and "documentary materials." The definition of "documentary materials" explicitly includes "materials upon which information is recorded, and includes . . . mechanically, magnetically or electronically recorded cards, tapes, or discs."[236] The physical hardware of a BBS certainly falls within this definition. In addition, the sort of information

234. PPA Legis. Hist., *supra* note 141, 1980 U.S.C.C.A.N. at 3956.
235. *Id.*
236. 42 U.S.C. § 2000aa-7(a).

stored on BBS system hardware appears to fall within the definition of "work product materials," described as "mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored, or created such material."[237] A person who has spent a significant amount of time on a BBS should be readily familiar with the fact that BBSs have a remarkably liberating effect on the opinions, theories, and mental impressions of BBS users. Under these statutory definitions, the seizure of BBS system hardware falls within the PPA.

The PPA does not create any additional burdens to securing a warrant where the target of the warrant is a suspect in a criminal offense.[238] For example, the PPA would not provide any special protection to a journalist under investigation for murder. However, the suspect exception does not apply where the only relevant offense is "the receipt, possession, communication, or withholding" of the materials sought in the search, or of the information contained therein.[239] This provision is of enormous significance to BBSs subject to searches aimed at uncovering evidence related to charges of computer software piracy, the distribution or possession of pornographic materials, or the distribution of copyrighted photographic, audio, or textual material. Since each of these charges consist of the receipt, possession, distribution, or communication of the materials sought, the government may not invoke the suspect exception in order to circumvent the PPA.

It is important to note that the PPA does not permit an aggrieved party to suppress the evidence obtained as a result of a search.[240] If a search or seizure performed in violation of the PPA uncovers incriminating information, the aggrieved party's exclusive remedy is a civil suit for damages. The party cannot suppress such information in later judicial proceedings merely because the information was discovered in violation of the PPA.

D. Politically and Sexually Oriented Materials

The revolution in computer communications has had immediate and far-reaching effects in the fields of politics and sexuality. Computer communications have politically empowered vast numbers of individuals

237. 42 U.S.C. § 2000aa-7(b)(3).
238. 42 U.S.C. § 2000aa(a)(1), (b)(1).
239. *Id.*
240. 42 U.S.C. § 2000aa-6(e).

by providing an effective means of political organization and communication. In the realm of sexuality, adult-oriented CD-ROMs and digitized photographs have been among the first and most popular products to utilize these technologies. In fact, sexually oriented materials account for twenty percent of current sales of interactive media titles, and sexual conferences remain the most popular on the Internet and local BBSs.[241] Computer systems that include materials of a sexual nature have received an extremely high level of attention from the government,[242] and computer systems with a political component have attracted attention from the government and private litigants hoping to examine their contents.

Materials of a sexual or political nature implicate the First Amendment right to freedom of expression. As a result, both the Fourth Amendment and the PPA provide enhanced protection to politically and sexually oriented computer systems in order to ensure that searches and seizures of these systems will not stifle free expression.

The Supreme Court has emphasized repeatedly that when a search or seizure intrudes onto unpopular or offensive visual or printed matter, courts must review Fourth Amendment issues with the utmost care. This extra level of care results from the Court's concern that searches and seizures can be used as a means to suppress objectionable books, magazines, films and other media. "History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."[243]

A 1980 case involving an FBI search of adult films held that: "When the contents of the package are books or other materials arguably protected by the First Amendment, and when the basis for the seizure is disapproval of the message contained therein, it is especially important that [the Fourth Amendment's warrant] requirement is scrupulously observed."[244] In another case, the Court addressed the limitations on the scope of a search and seizure of records taken from a regional Communist

---

241. *Most Popular Newsgroups (April 1994)*, WIRED, Aug. 1994, at 36 (four of the seven most popular Internet newsgroups are sex-related); Kenichi Murakami, *CD-ROM Sales Build on Techno-Erotica*, NIKKEI WEEKLY, July 25, 1994, at 11.

242. *See* David Landis, *Sex, Laws & Cyberspace*, USA TODAY, Aug. 9, 1994, at 1D; *see also supra* note 205.

243. United States v. United States Dist. Court, 407 U.S. 297, 314 (1972).

244. Walter v. United States, 447 U.S. 649, 655 (1980).

party headquarters, holding that "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain."[245] The Court has been explicitly skeptical of the ability of law enforcement officers to stay within the scope of the warrant when the officers are motivated by disapproval of the sexual or political content of the materials sought.[246]

At the very least, these cases establish that the Fourth Amendment requires courts to examine searches and seizures of politically and sexually oriented computer systems with extreme care to ensure that the search was adequately justified, that the warrant was sufficiently particular, and that the officers executing the warrant stayed within the scope of the warrant. These cases also indicate that whenever disapproval of the content of the materials stored on a computer system motivates a search or seizure of a politically or sexually oriented computer system, the government has the additional burden of affirmatively demonstrating that the "procedures leading to [the] issuance [of the warrants] and surrounding their execution were adequate to avoid suppression of constitutionally protected publications."[247]

If courts hold, as they should, that BBSs fall within the PPA's definition of disseminators of public communication, politically or sexually oriented BBSs will also enjoy the protection of the PPA.[248] But should courts decline to place BBS within the PPA, the scrupulous and exacting constitutional analysis afforded to sexually and politically oriented material will become particularly valuable.

CONCLUSION

Existing law provides an effective framework for protecting personal privacy and civil liberties from intrusive searches and seizures of

245. Stanford v. Texas, 379 U.S. 476, 485 (1965).

246. *See* Marcus v. Search Warrant, 367 U.S. 717, 729 (1961) (noting that the discretion given to officers to determine what falls within the scope of a warrant creates a "serious hazard of suppression of innocent expression"); *Stanford*, 379 U.S. at 485 ("The constitutional impossibility of leaving the protection of those freedoms to the whim of the officers charged with executing the warrant is dramatically underscored by what the officers saw fit to seize under the warrant in this case.")

247. *Marcus*, 367 U.S. at 731, *quoted in Stanford*, 379 U.S. at 486 n.18.

248. *See supra* parts I.C, III.C (discussing the PPA).

computers and computer storage facilities. As with any new technology, computers require courts to develop a consistent line of case law and statutory interpretation in a completely new context. Effective protection of computer privacy requires neither new statutory enactments nor the development of new Fourth Amendment doctrines. Foresighted constitutional doctrines and statutes already exist. However, these tools are somewhat obscure and have not been fully developed by the courts.

Five basic principles emerge: (1) The Fourth Amendment affords computer storage the highest expectation of privacy; (2) The *Tamura* rule should govern the scope of searches and seizures of all forms of computer data; (3) Government searches and seizures of computers motivated by disapproval of the content of the information sought must be subjected to the most exacting constitutional scrutiny; (4) The ECPA limits the ability of the government and private parties to obtain private computer communications; (5) The PPA places strict limitations on government attempts to seize the system hardware of computer BBSs or to shut them down altogether.

The Fourth Amendment provides the cornerstone for protecting the personal privacy of computer users. Little doubt exists that computer data will be entitled to the highest expectation of privacy. A typical home or office computer is an archetypal repository of highly personal information, and as such merits the highest level of Fourth Amendment protection. Existing cases recognize this fact, and establishing a high expectation of privacy is unlikely to be a troublesome question in future cases.

Once courts widely recognize this high expectation of privacy, the most significant question involves the permissible scope of a search or seizure. The *Tamura* rule, developed by the Ninth Circuit to resolve the troublesome Fourth Amendment question of how to limit searches of irrelevant documents that are intermingled with relevant documents, perfectly anticipates the problems posed by searches and seizures of computer data. The *Tamura* rule, though still obscure, has been praised in the case law and commentary. It provides an effective balance between the privacy needs of the individual and the needs of law enforcement officers. The rule anticipates the exigent circumstance that computer data can be erased or altered rapidly and recognizes that the separation of relevant from irrelevant information may be a time consuming process that officers may have to perform off-site. However, once computers and their storage media are removed from the control of the suspect, all exigent circumstances cease to exist. At this point, magistrates or other

neutral officials should supervise the methods used to sift through massive quantities of computer data. Wooden application of the closed container rule to computer storage fails to recognize the qualitative and quantitative differences between the intrusiveness of searches of computer storage and searches of the simple physical items around which the closed container rule developed.

Existing Fourth Amendment doctrine also requires that searches motivated by disapproval of the content of the information sought must be subjected to "scrupulous" constitutional analysis. Law enforcement personnel and courts must minimize the intrusiveness of searches and seizures of stand-alone computers, networks, and multi-user systems when the search or seizure is motivated by the sexual or political content of these systems. Regardless of the offensiveness of the content of these systems, Supreme Court authority demands that the warrant requirement and the particularity and overbreadth doctrines be "scrupulously" observed in order to minimize the intrusive effect of searches on protected expression.

For computer networks and multi-user systems, the ECPA supplements the protections of the Fourth Amendment. Unlike the Fourth Amendment, which applies only to searches and seizures conducted on behalf of the government, the ECPA prohibits private individuals from intruding into private computer communications. By requiring that searches of computer communications be conducted with prior judicial approval, and by limiting the length and intrusiveness of monitoring activities, the ECPA helps ensure the privacy of an individual's computer communications. The ECPA's failure to protect public computer communications is understandable. The government should be able to obtain computer files or transmissions that are otherwise freely available to the other users of a particular computer system. The ECPA's ordinary course of business exception is likely to generate the most controversy. If applied in keeping with the plain language of the statute, the ordinary course of business exception will not permit employers or computer system operators to engage in random general monitoring of system users. However, in order to protect computer communications effectively, it is crucial that courts not hesitate to suppress evidence obtained in violation of the ECPA.

The PPA has been an obscure and seldom applied statute since its enactment in 1980. However, the explosion in the popularity of computer bulletin boards and other on-line communications systems will require this statute to emerge from its dormancy and perform its intended function of

protecting those who disseminate their personal, political, and social views to others in their community. Computer bulletin board systems are a vital and growing medium for individual expression and social discourse. BBSs fall within the scope of the PPA and deserve its full protection. The PPA guarantees that government officials will have to utilize subpoenas or voluntary methods of compliance when seeking the system hardware and stored files of a BBS. In addition, First Amendment case law creates substantial obstacles to the compelled disclosure to the government and private parties of user and membership lists of BBSs.

Taken together, these statutory and constitutional provisions can provide adequate protection to information stored on computers. Despite initial fears that existing laws failed to anticipate the extraordinary role that computers play in everyday life, no major additions to statutory or constitutional law are necessary to adequately protect the privacy of computer users. These protections effectively balance the privacy needs of individuals against the needs of law enforcement authorities to occasionally search, seize, or monitor private computer files and communications. Courts must keep this balance in mind when applying the Fourth Amendment, the ECPA, and the PPA to the novel context of computers. Case law has not yet resolved most of the key issues presented by computer searches. Adequate protection will develop only if courts and law enforcement officers recognize the quantitative and qualitative differences between computers and other repositories of personal information, and only if courts realize the potential of searches and seizures of computers and computer data to intrude into all aspects of an individual's professional and personal life.