Oklahoma Law Review

Volume 53 | Number 1

1-1-2000

Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet

Amy E. Wells

COMMENT

Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet

He that would make his own liberty secure must guard even his enemy from oppression; for if he violates this duty he establishes a precedent that will reach to himself.[1]

I. Introduction

For modern individuals, cyberspace is the "new frontier." Increasingly, it has become the realm in which business is conducted, friendships are cultivated, and information is exchanged. Unlike all other uncharted territories, however, cyberspace has no physical geography; no territorial boundaries exist. Largely for this reason, traditional legal doctrines appear ill equipped to deal with contemporary problems that originate in cyberspace. In all likelihood, the immensity and rapid growth of cyberspace has already outstripped the ability of the law to keep pace.[2] Only through careful legislative initiatives and restrained judicial decision making can the law prove fit for dealing with the challenges created by cyberspace's information explosion.

Modern American society is robed in the Constitution and steeped in the rule of law. This should remain the state of affairs. However, sweeping technological advances often force the law to adapt. Communication via cyberspace has spurred some of the most dramatic societal changes in history. Today, estimates of Internet usage stand at about 67.5 million persons worldwide.[3] By the year 2003, researchers expect that there will be roughly 350 million Internet users.[4]

The exponential growth in the Internet user population underscores the sense of urgency with which those in the legal community must approach the law's ability to respond to future Internet problems. Concerns over the proper legal analysis to apply to issues of jurisdiction, privacy, and intellectual property are gaining increasing attention, as scholars and courts alike grapple with the prolific demands created by cyberspace.[5]

---

1. Thomas Paine, Dissertation of First Principles of Government, *in* 2 THE COMPLETE WRITINGS OF THOMAS PAINE 588 (Philip S. Foner ed., 1945).

2. *See* Anne M. Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 COMMLAW CONSPECTUS 63, 64 (1995).

3. *See Viruses' Economic Drain*, PC MAG., Sept. 1, 1999, *available in* 1999 WL 6782125.

4. *See* Phil Harvey, *LookSmart Promises to Clean Up the Clutter on the Internet*, UPSIDE MAGAZINE, Oct. 1, 1999, at 71, 71.

5. *See generally* Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181 (1995).

Like all other areas, criminal law must adapt to keep pace with advancing technology. Dealing with cyber-crime presents particularly difficult problems, in part because the choices which are made there can affect so many other areas of law.

This comment explores the uneasy application of the United States Constitution's Fourth Amendment search and seizure law to Internet crimes. This comment frames the analysis within the problem of child pornography. Part II provides a general introduction to the problem of child pornography on the Internet. Part III provides an overview of attempts by Congress to combat child pornography by statute, and recognizes the problem of statutory construction, which courts face. Additionally, Part III highlights law enforcement efforts at both the domestic and international level. Part IV discusses the Fourth Amendment and its application to Internet communications generally. Part V addresses the Tenth Circuit's attempt to apply Fourth Amendment analysis to electronic communications. Part VI pays tribute to the privacy concerns at stake in the context of Internet searches. Finally, this comment proposes that existing Fourth Amendment analysis can survive the societal transformation attributable to the rise of the Internet if the legal community makes a concerted effort to understand all that is at stake.

II. The Problem: Child Pornography on the Internet

The market for child pornography, unfortunately, is not new. Before computers, trading child pornography was a more personal endeavor. Consumers of child pornography either had to know each other or seek out an underground network that exchanged pictures and videos through the mail or in person.[6] Thus, access to child pornography was limited. However, the advent of the Internet and the increasing sophistication of computer technology in general has allowed distributors and consumers of child pornography to become more organized. The new medium has facilitated communication, making child pornography a global industry.[7]

Commentators note a number of reasons for the proliferation of child pornography on the Internet.[8] First, pornographic material depicting children in sexual situations is easily accessible on the Internet;[9] if one has a computer and is connected to the Internet, one has access to child pornography.[10] For example, traders in child pornography can visit electronic shops, browse through pornographic images, use their credit cards to purchase images they want and download their selections to either their hard drive or a floppy disk.[11] There are also private networks where pedophiles share sordid stories of abuse and swap pornographic pictures.[12] Also, electronic "chat

6. *See* Jennifer Stewart, *If This Is the Global Community, We Must Be on the Bad Side of Town: International Policing of Child Pornography on the Internet*, 20 HOUS. J. INT'L. LAW 205, 213 (1997).

7. *See id.* at 212; *see also* Lesli C. Esposito, Note, *Regulating the Internet: The New Battle Against Child Pornography*, 30 CASE W. RES. J. INT'L L. 541, 542 (1998).

8. *See* Stewart, *supra* note 6, at 211.

9. *See id.* at 213.

10. *See id.*

11. *See* John Henley, *The Observer Campaign to Clean Up the Internet: Hackers Called in as Cybercops to Drive Out Porn*, OBSERVER, Sept. 1, 1996, *available in* 1996 WL 12065705.

12. *See id.*

groups" provide easy access where child "pornography can be exchanged more or less anonymously."[13]

Second, advances in computer technology have increased the ability to produce child pornography.[14] Traders in child pornography can use computer scanners to input images onto the Internet from other sources.[15] Additionally, "video-capture" devices exist, which can pick up a still frame from the television, video camera, or VCR and input the image into the computer.[16] Similarly, one can use computer video cameras to record "live action," allowing full color video and sound to be recorded and transmitted via the Internet.[17] Similarly, much of the child pornography found on, or traced through, the Internet has come to be called "virtual child pornography."[18] Virtual pornography takes many different forms. At one end of the spectrum, an image is created entirely without the use of an actual child.[19] Other virtual images are composed of numerous pictures of adults and children morphed[20] together.[21]

Additional technological advances have revolutionized the distribution of child pornography.[22] Consumers and dealers of child pornography can exchange material on floppy disks or through the Internet, as opposed to using the mail or meeting in person.[23] The quality of digital images on the Internet is also superior to and lasts longer than photographs.[24] The Internet has made it possible to "mass market" child pornography with virtually no overhead, thus increasing consumer demand for the material.[25]

Third, the Internet provides anonymity.[26] For example, a person can establish a bulletin board, and use it to exchange sexual interests in children, without a license or registration.[27] Additionally, while commercial online service providers use adults to monitor online discussions, news groups and chat groups with the "alt" prefix are usually not regulated in this way.[28] A person can reroute e-mail and graphic images

---

13. Stewart, *supra* note 6, at 213.

14. *See id.* at 213-14.

15. *See id.* These scanners change photographic images into digital form, which may then be saved as files on a computer hard drive or floppy disk. *Id.* at 214.

16. *See id.*

17. *See id.*

18. *See* Debra D. Burke, *The Criminalization of Virtual Child Pornography: A Constitutional Question*, 34 HARV. J. ON LEGIS. 439, 440-41 (1997).

19. *See id.* at 440.

20. "Morphing," also known as "metamorphosing," is a process that allows a computer to fill in the area between dissimilar objects in order to produce a combined image. *See id.* at 440 n.5.

21. *See* Wendy L. Pursel, *Computer-Generated Child Pornography: A Legal Alternative?*, 22 SEATTLE L. REV. 643, 644 (1998).

22. *See* Stewart, *supra* note 6, at 213.

23. *See id.*

24. *See id.* at 214.

25. *See id.* at 214-15.

26. *See id.* at 215.

27. *See id.*

28. *See* Mark Clayton, *"Off-Line" Hazards Lie in Web's Links, Lures*, CHRISTIAN SCI. MONITOR, Aug. 29, 1996, at 10. The "alt" prefix designates a newsgroup as alternative and unofficial. *See also*

through multiple nations so that the origin of the file is virtually undetectable.[29] Further, Internet users commonly use nicknames or aliases, which make it more difficult for authorities to identify them.

With the ascendancy of a now global child pornography industry, largely attributable to increasing Internet use, the criminal law has had to be expanded in some areas and readapted in others. As the balance of this comment seeks to illustrate, this situation has created challenges both for legislators and the courts as well as law enforcement officials.

III. Attempts to Combat the Problem

The legislative and executive branches of the United States government have grappled with methods of apprehending and convicting individuals who create or disseminate child pornography on the Internet.[30] Effectively combating Internet crime requires the coordination of local, national, and international resources. This section explores the development of laws aimed at eradicating child pornography. Additionally, this section examines specific law enforcement methods used to identify, apprehend and prosecute persons engaged in the exchange of child pornography over the Internet. Finally, brief attention is dedicated to the international community's response to the problem of child pornography.

A. Statutory Response

Criminalization of the possession and distribution of child pornography in the United States has been evolving over several decades. Early legislative initiatives were ineffective in dealing with the problem of child pornography in the context of computer technology. The Federal Protection of Children Against Sexual Exploitation Act, enacted in 1978, prohibited the production of "sexually explicit" material using a child under the age of sixteen, if such material will travel or has traveled in interstate commerce.[31] However, because this law reached only the commercial exchange of child pornography, it did not prohibit trading or giving away the material, even if sent through the United States mail.[32] To correct this problem, Congress passed the Child Protection Act (CPA) in 1984, eliminating the requirement of a commercial transaction.[33] The CPA recognized an earlier decision by the Supreme

---

JOHN R. LEVINE ET AL., THE INTERNET FOR DUMMIES 218, 225 (5th ed. 1998) (recognizing that some Internet users take advantage of the anonymity and lack of regulation).

29. *See* LEVINE, *supra* note 28, at 224.

30. In 1999, President Clinton issued an executive order establishing a working group to address unlawful conduct, including child pornography, involving the use of the Internet. *See* Exec. Order No. 13,133, 64 Fed. Reg. 43,895 (1999).

31. Protection of Children Against Sexual Exploitation Act of 1977, Pub. L. No. 95-225, § 2252(a), 92 Stat. 7, 7-8 (1978) (codified as amended at 18 U.S.C. § 2252 (1994)).

32. *See* ATTORNEY GENERAL'S COMM'N ON PORNOGRAPHY, U.S. DEP'T OF JUSTICE, FINAL REPORT 67, 133 (1986).

33. *See* Child Protection Act of 1984, Pub. L. No. 98-292, § 4, 98 Stat. 204, 204-05 (1986) (codified as amended at 18 U.S.C. § 2252 (1994)). Additionally, the 1984 Act changed the definition of a minor to a person under the age of eighteen. *See id.*

Court in *New York v. Ferber*,[34] which made obsolete the obscenity test previously announced by the Supreme Court in *Miller v. California*,[35] at least in the context of child pornography. Finally, in 1986 Congress passed the Child Sexual Abuse Act, which banned the production and use of advertisements for child pornography.[36]

Congress first addressed the problem of the relationship between child pornography and computer technology with the enactment of the Child Protection and Obscenity Enforcement Act of 1988.[37] This law criminalizes the use of computers to transmit advertisements for, or visual depictions of, child pornography.[38] However, as computer technology rapidly evolved, this statute became less effective. Early legislative prohibitions against child pornography in the United States were aimed at addressing the harm done to children by the production and distribution of pornographic material.[39] Consequently, these statutes utterly failed to recognize that pornographic images could be digitally created without actually involving children.[40] To correct this and other weaknesses, Congress enacted the Child Pornography Protection Act (CPPA) in 1996.[41] For the first time, federal law defined child pornography to include "computer" or "computer-generated image(s) or picture(s)" of minors engaged in sexually explicit conduct.[42]

Although the CPPA provides a stronger legal basis for the conviction of those exchanging child pornography on the Internet, commentators and courts alike have found problems with the Act. At least one court has ruled that the statute is "impermissibly vague and overbroad."[43] In *United States v. Hilton*, the defendant was

---

34. 458 U.S. 747 (1982).

35. 413 U.S. 15, 24 (1973). In *Miller*, the Court held that pornography found to be obscene by contemporary community standards, does not enjoy the protection of the Fourth Amendment. *See id.* at 36. Essentially, the *Miller* test for determining obscenity is: (a) whether "the average person applying community standards" would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. *Id.* at 24. In *Ferber*, the Court found that the Miller obscenity standard did not apply to child pornography because child pornography is per se obscene. *See Ferber*, 458 U.S. at 755-56.

36. Child Sexual Abuse and Pornography Act of 1986, Pub. L. No. 99-628, § 2, 100 Stat. 3510, 3510-11 (1989) (codified at 18 U.S.C. § 2251(c) (1994)).

37. Child Protection and Obscenity Enforcement Act of 1988, Pub. L. No. 100-690, §§ 7511-7513, 102 Stat. 4485, 4485-87 (1990) (codified at 18 U.S.C. §§ 2251(c), 2252(a), 2256, 2251A (1994)).

38. *See* 18 U.S.C. § 2252(a)(1)-(2).

39. *See* David J. Loundy, *Who Hasn't Noticed? Child Porn Already Illegal*, 144 CHI. DAILY L. BULL., May 14, 1998, *available in* Westlaw, 5/14/98 CHIDLB 6.

40. *See id.*

41. *See* Child Pornography Protection Act of 1996, Pub. L. No. 104-208, 1996 U.S.C.C.A.N. (110 Stat.) 26 (codified as amended at 18 U.S.C. § 2256 (1994)).

42. *Id.*

43. United States v. Hilton, 999 F. Supp. 131, 137 (D. Me. 1998), *rev'd*, 167 F.3d 61 (1st Cir. 1999). The United States Supreme Court has held that a statute which is impermissibly vague is unconstitutional because such a malady may inhibit the exercise of the freedoms protected by the First Amendment. *See id.* at 135 (citing Grayned v. City of Rockford, 408 U.S. 104, 109 (1972). To avoid being deemed "vague," a statute must "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage

charged with possessing child pornography. He moved to dismiss the charges brought against him under the CPPA, claiming that the statute violated his First Amendment rights.[44] The defendant argued that section 2256(a)(5)(B) of the CPPA, in conjunction with the definition of child pornography set forth in section 2256(8)(B)[45] did not clearly identify the prohibited conduct. More specifically, he argued that the definition of "child pornography," which includes visual depictions that *appear* to be of minors engaged in sexually explicit conduct, is too subjective to enable ordinary people to know what conduct is prohibited.[46]

The *Hilton* court applied the doctrines of "vagueness" and "overbreadth," emphasizing that a statute suffering either malady inhibits the exercise of freedom of speech protected by the First Amendment and is therefore unconstitutional.[47] In order to avoid being characterized as impermissibly vague, a statute must "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement."[48] The court concluded that "[t]he CPPA's definition of 'child pornography' creates substantial uncertainty for viewers presented with materials depicting post-pubescent individuals, for the determination as to whether those individuals have yet reached eighteen years of age will often not be easy or clear."[49] Additionally, the court noted that the classification of computer generated images according to this subjective standard would be equally difficult.[50] For these reasons, the court struck down the statute as unconstitutionally vague.[51]

The *Hilton* court also embraced the defendant's claim that the statute was impermissibly overbroad, noting that a statute may be overbroad if it encompasses conduct that is constitutionally protected.[52] The court found that the definition of "minor" under the statute, together with its role in defining "child pornography," may impact a large amount of adult pornography featuring youthful looking adults.[53] Because the statute's subjective language would chill expression involving adults, the court held that the statute was unconstitutionally overbroad.[54]

---

arbitrary and discriminatory enforcement." *Id.* (citing Kolender v. Lawson, 461 U.S. 352, 357 (1983)). Additionally, if a statute prohibits constitutionally protected conduct, it may be deemed overbroad as well. *See id.* (citing *Grayned*, 408 U.S. at 114). However, a statute regulating expressive conduct will not be rendered unconstitutional unless its overbreadth is not only "real but sustainable as well." *Id.* at 137 (citing Osborne v. Ohio, 495 U.S. 103 (1990)).

44. *See id.* at 132.

45. Section 2256(8)(B) defines "child pornography" as including visual depictions which "appear to be of a minor" as well as those which are of a minor. 18 U.S.C. § 2256(8)(B).

46. *See Hilton*, 999 F. Supp. at 136.

47. *See id.* at 135.

48. *Id.* (citing Kolender v. Lawson, 461 U.S. 352, 357 (1983)).

49. *Id.* at 136.

50. *See id.*

51. *See id.*

52. "[W]here a statute regulates expressive conduct, the scope of the statute does not render it unconstitutional unless its' overbreadth is not only real, but substantial as well . . . ." *Id.* (citing Osborne v. Ohio, 495 U.S. 103, 112 (1990)).

53. *See id.* at 137.

54. *See id.*

The approach to the CPPA asserted in *Hilton* does not enjoy universal support.[55] In fact, the First Circuit has since overruled the decision.[56] However, the case serves as an illustration of the unique problem of statutory construction, which courts face in attempting to strike a just balance between maintaining constitutional protection of speech and combating the problem of child pornography.

Commentators in the legal community have also waged a fervent attack on the CPPA. One observer charges the CPPA with being "reactionary legislation, passed in the name of regulating the electronic frontier" with its primary function being to threaten constitutional rights.[57] Another applauded the result reached by the lower *Hilton* court, stating that laws in existence prior to the CPPA were sufficient to prevent the harm caused by the distribution of child pornography online.[58]

B. Law Enforcement Efforts

Law enforcement activities directed at the problem of child pornography on the Internet take several different forms. Wiretapping and tips from informants are utilized, as are subpoenaed records of online transmissions from Internet service providers (ISPs).[59] Currently, the most widely used method to track and apprehend traders in child pornography is undercover activity by law enforcement.[60]

The Federal Bureau of Investigation's "Innocent Images" initiative involves coordinating nationwide undercover investigations of child pornographers.[61] Innocent Images grew out of a 1995 investigation into the disappearance of a ten-year-old boy.[62] Inquiry into two suspects linked to the boy's disappearance revealed that the suspects as well as other adults were routinely using computers both to transmit images of minors showing frontal nudity or sexually explicit conduct and to lure minors into sexual activities.[63] To identify those individuals who are victimizing children, the FBI formed a task force composed of FBI agents and other federal, state, and local investigators who go online in an undercover capacity, posing as either

55. *See* Loundy, *supra* note 39.

56. *See* United States v. Hilton, 167 F.3d 61, 77 (1st Cir. 1999) (finding the CPPA to be neither unconstitutionally vague nor overbroad because the statute targets only a narrow class of images and the ordinary consumer of sexually explicit materials is given adequate notice of the kinds of images to avoid).

57. Loundy, *supra* note 39.

58. *See* Brenda M. Simon, *First Amendment Internet Crime Statutes: Child Pornography. United States v. Hilton*, 14 BERKELEY TECH. L.J. 385, 401 (1999).

59. *See* Michael Grunwald, *Global Internet Child Porn Ring Uncovered*, WASH. POST, Sept. 3, 1998, at A12, *available in* 1998 WL 16553624.

60. *See id.* See *United States v. Wilson*, 182 F.3d 737, 739 (10th Cir. 1999), *United States v. Katz*, 178 F.3d 368, 369 (5th Cir. 1999), and *United States v. Upham*, 168 F.3d 532, 533 (1st Cir. 1999), as examples of the use of undercover agents to apprehend child pornographers who use the Internet.

61. *See Proliferation of Child Pornography on the Internet: Hearings Before a Subcomm. of the Senate Comm. on Appropriations*, 105th Cong. 1 (1998) (statement of Louis J. Freeh, Director, FBI).

62. *See id.* (discussing the disappearance of George Stanley Burdynski, Jr., in Prince George's County, Maryland).

63. *See id.*

young children or as sexual predators.[64] In 1998, the FBI reported that its Innocent Images investigation had generated 184 convictions since its inception.[65]

Although undercover detection appears to have been effective thus far, as child pornographers become more savvy over time, the method will likely wane in its effectiveness. Of course, it is difficult to conceive of circumstances that would make undercover operations obsolete. Given the annual increase in funding to such programs, it is unlikely that the FBI will ever abandon the method.

The FBI has also introduced efforts to limit the use of encryption technology as a method of tracking perpetrators of Internet crimes, including child pornographers.[66] This has spurred a heated debate evident in both legal scholarship and the writings of public action groups, which fear the privacy implications that such limits could have.[67] As one scholar explains, the study of encryption, or *cryptography*, is an obscure field of mathematics in which individuals make and break codes using mathematical algorithms.[68] A cryptosystem is a collection of algorithms that enables an individual to encrypt a message by transforming it from its original form into an undecipherable one.[69] An individual who later receives the message will be unable to read it without first *decrypting* the message.[70]

The technical details of the various types of cryptographic systems are very complex and beyond the scope of this comment. However, the practical uses of encryption are important to note. Businesses, banks, and the government are the most dominant users of encryption technology for obvious reasons.[71] Safeguarding trade secrets, financial records, and information relating to the nation's security are all good reasons to allow the encryption of computer data.[72] Along those same lines, individuals also have an interest in keeping various aspects of their lives shielded from the public at large. But some argue that allowing everyone to use encryption protects criminals from being detected.[73] Others passionately support the right of *all* individuals to have access to the best encryption technology.[74] In other words, in an

64. *See id.*

65. *See id.* (noting that since March 1997 the number of search warrants executed increased 62%, the number of indictment increased 50%, and the numbers of arrests and convictions increased 57% and 45% respectively).

66. *See id.* (reporting on the problem of sexual predators who use encryption and the need of law enforcement to have access to such files and the technology to decode them).

67. *See* Bill Pietrucha, *ACLU Calls Encryption Actions Nightmare For Privacy*, NEWSBYTES NEWS NETWORK, Sept. 12, 1997, *available in* 1997 WL 13910671 (asserting that the FBI is demanding "a front door key to every American's house, just in case a criminal happens to be hiding out somewhere").

68. *See* Kenneth P. Weinberg, *Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)*, 5 J. INTELL. PROP. 667, 673 (1998) (explaining that an algorithm may be used to transform information from "plaintext" to "cyphertext" and visa versa).

69. *See id.* at 674.

70. *See id.*

71. *See id.* at 676-79.

72. *See id.* at 676.

73. *See id.* at 681.

74. *See generally Americans for Computer Privacy* (visited Apr. 4, 1999) <http://www.computerprivacy.org>.

open, democratic society, the rights of the individual sometimes supersede those of society at large.

The success of law enforcement officials at both the state and federal levels in tracking and apprehending the consumers and traders of child pornography will depend greatly on their ability to stay up-to-date with the rapid advancement of computer technology. However, the efficacy of law enforcement also hinges on the *license* given them by legislation and judicial decisions.

C. The International Arena

At the international level there is no formal treaty that establishes an obligation between nations to pursue child pornographers.[75] However, due to the near universal desire to protect children, there is a significant degree of international cooperation. The rise of Internet use, not surprisingly, runs concomitant to the intensification of cooperative efforts. Illustrative of this fact is the recent raid on roughly two hundred suspected members of an Internet child pornography ring, which called themselves the "Wonderland Club."[76] The sweeps were conducted simultaneously on targets in the United States, Australia, and twelve European countries based on evidence collected and shared by law enforcement officials in those countries.[77]

Aside from the cooperation of domestic law enforcement at the international level, certain international organizations and commercial enterprises have enlisted in the battle against child pornography.[78] Interpol (International Criminal Police Organization)[79] actively promotes the detection and conviction of those who engage in the sexual exploitation of children.[80]

Some efforts have been made to encourage self-censorship by Internet service providers (ISPs).[81] ISPs can simply refuse to sell space to anyone they know to be providing child pornography.[82] In the United States, it is unlikely that this option will succeed, largely because of federal legislation that relieves ISPs from liability.[83] Ironically, at least one court has ruled that a server which takes on the responsibility of self-regulation may be subjected to even greater liability if it falls short of this endeavor.[84] However, the trend in other nations seems different.[85]

---

75. However, the United Nations Convention on the Rights of the Child, which entered into force in 1990, defines as a part of international law universal children's rights and specifically addresses child pornography. Under the Convention, all state Parties are required to "take all appropriate national, bilateral and multilateral measures to prevent . . . (c) the exploitative use of children in pornographic performances and materials." *See* Esposito, *supra* note 7, at 59-61 (citing Convention on the Rights of the Child, G.A. Res. 25, U.N. GAOR, 44th Sess., Supp. No. 49, at 171, U.N. Doc. A/44/736 (1989)).

76. *See* Grunwald, *supra* note 59, at A12.

77. *See id.* (listing the countries involved in the operation and describing the procedures used).

78. *See* Stewart, *supra* note 6, at 228-29.

79. *See id.* at 229.

80. *See id.*

81. *See id.* at 230.

82. *See id.*

83. Communications Decency Act of 1996, 47 U.S.C. § 223 (Supp. III 1997). The Communications Decency Act (CDA) states that no person shall be liable for violating the Act "solely for providing access or connection to or from a facility, system or network not under that person's control." *Id.* § 223(e)(1).

84. *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *5 (N.Y.

Nongovernmental organizations (NGOs), which act at the international level, are also fighting the battle against child pornography.[86] These groups exist for various reasons ranging from commercial to humanitarian and political.[87] One NGO has directed its efforts towards detecting pedophiles and child pornographers on the Internet by establishing a "cybercop" unit made up of undercover agents who police the Internet.[88]

Inherent to the goal of pursuing child pornographers who use the Internet to exchange their wares is the need for cooperation on the international level.[89] Hopefully, efforts by the various bodies will continue to develop efficacious methods to deal with the problem while keeping an eye on democratic values. The interest of the international community in apprehending child pornographers must be carefully balanced against the rights individuals enjoy in a democratic society. The respective states should come together with an understanding of their differences on such issues as privacy and freedom of speech. They must thoughtfully choose when compromises on such issues should and should not be made.

IV. Fourth Amendment Analysis — Responding to the Internet

The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures by the government and sets forth guidelines for granting search warrants:

> 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.[90]

In order to determine whether the reasonableness and warrant requirements of the Fourth Amendment apply to communications, it is first necessary to decide whether the inspection of such communications constitutes a "search." The task of defining

---

App. Div. May 24, 1995), *superseded by statute as stated in* Zeran v. America On Line, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (holding that 47 U.S.C. § 230 immunizes Internet service providers like AOL from liability for information that originates with third parties). The case revolved around an action for libel based on statements posted on a Prodigy bulletin board. The court found that since Prodigy "held itself out as an on-line service that exercised editorial control over the content of messages posted on its computer bulletin boards," it exposed itself to greater liability than other computer networks that made no such choice. *Id.* Ultimately, the court entered summary judgement for the plaintiffs.

85. In 1998, a Bavarian judge sentenced the former head of Compuserve Deutschland to two years in jail for distributing pornography involving animals and children since such material could be accessed via the Compuserve server. *See* Alan Cowell, *Head of German Web Sentenced for Pornography*, N.Y. TIMES, May 29, 1998, at A1.

86. *See* Stewart, *supra* note 6, at 234.

87. *See id.*

88. *See id.* at 235 (speaking of Norwegian Save the Children).

89. Of course, this is true of the general need to regulate all Internet crimes. *See generally* Michael Hatcher et al., *Computer Crimes*, 36 AM. CRIM. L. REV. 397 (1999).

90. U.S. CONST. amend. IV.

government action as a search, and thus subject to Fourth Amendment scrutiny, has largely been guided by Supreme Court decisions.[91] If government conduct constitutes a search, then it must be reasonable and pursuant to a valid warrant, barring an exception outlined *infra*.[92]

This section will chart the evolution of Fourth Amendment analysis as it highlights the law's response to social, political, and most importantly, technological change. What emerges from this review is troubling. Modern Fourth Amendment principles and guidelines are in many ways obsolete when superimposed over the computer data medium.

A. Background to Current Fourth Amendment Analysis

Throughout the earlier part of the twentieth century, the Supreme Court applied what some term a "property-based" standard when dealing with Fourth Amendment questions.[93] In *Boyd v. United States*,[94] recognized as the Court's first significant examination of the Fourth Amendment, the protection of property was found to lie at the heart of the Amendment.[95] In *Boyd*, a contracting firm was accused of claiming more cases of plate glass as exempt from customs duties than the firm had actually used.[96] The issue facing the Court was whether the government could subpoena the firm's papers to use against the firm. Justice Bradley, writing for the majority, found that the protection of an individual's property interest served to restrict "all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."[97] Thus, the Court found that the firm alone was entitled to possess the papers that the government sought, because the papers were the property of the firm.[98] Essentially, the Court found that an individual's private property interest outweighed the government's interest in prosecuting a crime.[99]

While this property-based paradigm survived for more than half a century, later decisions retreated from the absolute protection of property principle set forth in *Boyd*. Instead, the Supreme Court began to carve out a variety of "constitutionally protected area[s]."[100] This view of the Fourth Amendment permitted government agents to inspect any unprotected area without a warrant or probable cause. However, excluding

91. *See infra* text accompanying notes 93-106.

92. *See infra* text accompanying notes 180-191.

93. *See* Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1101-02 (1996).

94. 116 U.S. 616 (1886).

95. *See* Adler, *supra* note 93, at 1101; *see also* WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 3.1, at 105 (2d Student ed. 1992).

96. *See Boyd*, 116 U.S. at 618.

97. *Id.* at 630.

98. *See id.* at 631.

99. *See id.* at 631-32.

100. Hester v. United States, 265 U.S. 57, 59 (1924) (holding that an "open field" was not a constitutionally protected area); *see also* Lanza v. New York, 370 U.S. 139, 143 (1962) (finding that house, office, store, hotel room, and car were "protected areas" but that visitors' room of a jail was not).

a "few specifically established and well-delineated exceptions,"[101] official intrusion into a protected area required a warrant supported by probable cause.

The area-based model of Fourth Amendment analysis was applied in *Olmstead v. United States*,[102] where the Supreme Court addressed the necessity of a search warrant in the context of a wire tap.[103] In *Olmstead*, the Court held that using a wire tap to eavesdrop on phone conversations was not a "search" where the wires actually tapped were not a part of the defendant's home or office.[104]

To some, the *Olmstead* decision represents the inadequacy of the area-based approach to Fourth Amendment analysis in the context of electronic communications.[105] For example, one author examines the prospect of a "net-wide" search by government officials whereby a program could scan through millions of files, unbeknownst to computer owners, and report to the authorities the presence of only illegal files.[106] How would such an intrusion be characterized? A physical entrance into the home or business is not involved, but it seems that most observers would view the search program as an intrusion, even if illegal files were not discovered on their computers. However, under *Olmstead*, it is unclear how a court would rule. On the one hand, a court could find that the search program was not a search for Fourth Amendment purposes because the government did not physically enter the home or office; the government was merely *eavesdropping* using a device installed on a government computer in a distant city. On the other hand, a court could view the government action as more intrusive than that in *Olmstead*, and find that a search occurred, reasoning that the program essentially entered a person's home or office through their computer. This hypothetical illustrates the conceptual difficulties involved when attempting to apply outdated legal principles to new technology. The Supreme Court's subsequent rejection of *Olmstead*[107] was largely due to new ideas regarding the individual and technology, and therefore illustrates how, at its best, the law evolves to fit current circumstances.[108]

B. Modern Fourth Amendment Analysis and Its General Application to Computer Communications

1. Private Searches Are Not Protected

As a preliminary matter, it is important to recognize that the Fourth Amendment protects against unreasonable searches and seizures by the *government*.[109] Searches

101. Katz v. United States, 389 U.S. 347, 357 (1967).

102. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

103. *See* Sergent, *supra* note 5, at 1186.

104. *See Olmstead*, 277 U.S. at 464-65.

105. *See* Sergent, *supra* note 5, at 1187.

106. *See generally* Adler, *supra* note 93.

107. The Supreme Court later "conclude[d] that the underpinnings of *Olmstead* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." *Katz*, 389 U.S. at 353.

108. *See* Sergent, *supra* note 5, at 1186 (explaining that *Olmstead* "is a prime example of the inadequacy of the area-based approach for a society dependant upon electronic communications").

109. *See* LAFAVE & ISRAEL, *supra* note 95, § 3.2, at 117-18.

and seizures by private citizens or nongovernment actors may form the basis for redress, but it will not likely give rise to Fourth Amendment protection. The exception to this general rule is where a private entity acts as a government agent.[110] Determining whether a private individual is acting on behalf of the government involves answering several questions. First, did the government know about and encourage the intrusive conduct? Second, did the private actor intend to assist the efforts of law enforcement by conducting the search or was it to further his own ends? Third, did the government offer the private actor some type of reward?[111]

The courts have addressed the "private search" in the context of computer communication. In *United States v. Hall*,[112] the defendant took his computer to a repair service. A repairman viewed various files containing images of children engaging in sexually explicit acts. He then copied the incriminating files to a disk and helped law enforcement pursue the defendant. In *Hall*, the court held that the search conducted by the repairman was not covered by the Fourth Amendment; it was a private search.[113] In reaching this conclusion, the court reasoned that the search by the repairman was conducted pursuant to the maintenance work done in his position as employee.[114] Additionally, the government did not know the repairman would repair the defendant's computer, so it could not have instructed him to inspect the computer files.[115]

2. The "Reasonable Expectations" Test

In *Katz v. United States*,[116] the Supreme Court established the current approach to Fourth Amendment analysis. In *Katz*, the Court held that a "search" was within the meaning of the Fourth Amendment when government electronically listened to and recorded the defendant's words spoken into a telephone receiver inside a public telephone booth because these actions violated the defendant's privacy on which he justifiably relied.[117] Furthermore, the fact that the electronic device used by the government did not penetrate the wall of the phone booth had no constitutional significance whatsoever.[118] Since *Katz*, the Court focuses on an individual's "expectations of privacy" with respect to the area or object that was searched. Most importantly, *Katz* emphasized that "the Fourth Amendment protects people, not places."[119] Justice Harlan's concurring opinion became the basis for the Supreme Court's current two-part test to determine whether a given government inspection constitutes a search.[120] First, the Court must determine whether government action

110. *See id.* at 118.

111. *See id.*; *see also* United States v. McAllister, 18 F.3d 1412, 1417 (7th Cir. 1994).

112. 142 F.3d 988 (7th Cir. 1998).

113. *See id.* at 993.

114. *See id.*

115. *See id.*

116. 389 U.S. 347 (1967).

117. *See id.* at 353.

118. *See id.* at 356-57.

119. *Id.* at 351. "What a person knowingly exposes to the public, even in his own home or office, 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." *Id.* at 351-52.

120. *See id.* at 361 (Harlan, J., concurring).

violated an individual's subjective expectation of privacy.[121] Second, if society recognizes that expectation as *reasonable*, then the inspection is a search and the protections of the Fourth Amendment apply.[122]

The "reasonable expectation of privacy" test is composed of both an objective and subjective prong. Consequently, the two-part test has been criticized as difficult to apply.[123] The subjective element of the test has been attacked because relying on a subjective notion of what is "private" can easily be defeated by an announcement by the government that something is not private.[124] In other words, as the great architect of the test himself said, "[o]ur expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present."[125] Perhaps because of this difficulty in application, the subjective prong has received little, if any, attention in the analysis of Fourth Amendment issues. Subjective notions of whether various forms of computer data are *private* will vary depending on the degree of an individual's technical knowledge. Often, the level of one's knowledge about computer data will be inversely related to their expectation of privacy in that data.

Similarly, the objective reasonableness prong of the *Katz* test has also been subjected to criticism. It has been suggested that a determination of objective reasonableness ultimately rests on a "value judgement" or a determination of how much privacy we, as a society, should enjoy.[126] Determining whether an individual's expectation of privacy in computer data is *objectively reasonable* is quite troubling. How much does society actually know about the vulnerability of Internet transmissions and computer files to being searched or intercepted? The answer is that it varies so greatly among persons that an objective measure is virtually impossible to conceptualize. Although some may argue that this difficulty exists in other contexts as well, such a shortcoming significantly affects the lives of real people, and thus should not be blindly accepted.

Due to the difficulty in applying the *Katz* test to computer information, courts often turn to earlier notions of privacy and have attempted to draw analogies to the new medium;[127] thus, it is helpful to revisit some of these earlier applications. The Supreme Court has held that the following activities do not constitute searches under the Fourth Amendment: canine sniffs of cars or luggage,[128] using electronic beepers to track vehicles,[129] subpoenaing bank records,[130] using undercover agents,[131] flying over residential property,[132] using a pen register to record numbers dialed on a

121. *See id.*

122. *See id.*

123. *See* LAFAVE & ISRAEL, *supra* note 95, § 3.2, at 125.

124. *See id.* at 126.

125. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

126. *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

127. *See infra* text accompanying notes 138-141.

128. *See* United States v. Place, 462 U.S. 696, 707 (1983). However, some states have granted greater protection under state constitutions. *See, e.g.*, State v. Pellici, 580 A.2d 710, 716 (N.H. 1990).

129. *See* United States v. Knotts, 460 U.S 276, 285 (1983).

130. *See* United States v. Miller, 425 U.S. 435, 441-43 (1976).

131. *See* United States v. White, 401 U.S. 745, 749 (1971).

132. *See* Florida v. Riley, 488 U.S. 445, 450 (1989); *see also* California v. Ciraolo, 476 U.S. 207,

telephone,[133] and rummaging through trash discarded at the curb for pickup.[134] Since these actions by law enforcement officials do not constitute searches, the protections of the Fourth Amendment do not apply. Law enforcement need not acquire a warrant to engage in these activities.

Conversely, courts have held other governmental actions clearly to be searches and thus protected by the Fourth Amendment. Generally, the use of electronic eavesdropping or wiretapping equipment are considered "searches," as are unconsented entrances into residential units.[135] Along this same vein, areas close to one's house (or "inside the curtilage") are also protected.[136] Individuals also retain a reasonable expectation of privacy in sealed first-class mail sent through the postal system.[137]

Analogies to these earlier notions of privacy are abundant in recent case law regarding computer technology. For example, in *United States v. Maxwell*,[138] the court equated an e-mail message with first-class mail and telephone conversations.[139] The court reasoned that in the cases of both first-class mail and telephone conversations, a party relies on an intermediary (either the post office or the telephone company) to relay the message to the recipient; however, a party maintains an expectation of privacy in the content of the message.[140] Similarly, the sender of e-mail relies on a service to deliver the message to the intended recipient, yet he retains an expectation of privacy in the content of the message.[141] *Maxwell* is illustrative of the emerging "analogical method." Since lawyers, judges, and legal scholars will play a role in developing the law in this area, they should cooperate to ensure that well reasoned, deliberate decisions are made when comparing situations involving computer technology to those earlier instances. Furthermore, if there is no analogy that "fits" in a particular case, lawyers, judges, and legal scholars must be willing to develop new applications of the "expectations test."

In addition to analogizing, courts applying the Fourth Amendment "expectations test" to cyberspace communications may rely on one of several analytical models. For example, one commentator notes that the nature of the system on which the particular communication is found should be a factor.[142] In other words, courts should look at whether a computer is a single user PC located in a private home, a multiuser system found in an office, or a public system maintained by a library or university.[143] Recently, in a trial of a Chicago man charged with possession of child pornography with intent to distribute, prosecutors argued that the defendant's e-mail proved his intent

---

213-14 (1986).

133. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).
134. *See* California v. Greenwood, 486 U.S. 35, 40-41 (1988).
135. *See* LAFAVE & ISRAEL, *supra* note 95, § 3.2, at 128-30.
136. *See id.* at 131-32.
137. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877).
138. 45 M.J. 406 (C.A.A.F. 1996).
139. *See id.* at 417.
140. *See id.* at 417-18.
141. *See id.*
142. *See generally* Sergent, *supra* note 5.
143. *See id.*

to distribute.[144] In response, the defense attorney pointed to the fact that others had access to defendant's computer and could have easily written the incriminating e-mail.[145] While the e-mails were permitted as evidence at trial, the court was not convinced that their mere existence proved that defendant intended to distribute the child pornography and he was ultimately acquitted of those charges.[146]

The multiuser system poses greater problems in determining the privacy issue.[147] According to one commentator, the threshold question is whether it is possible to have a legitimate privacy interest in information distinct from "ownership or control of the underlying storage media."[148] It has been suggested that in order to have a reasonable expectation of privacy in some types of data on a multiuser system, "the data must not knowingly be exposed to other users of the system and the system manager's ability to access the data must not constitute a disclosure" to a third party.[149]

This "nature of the system" approach focuses to some degree on the steps taken to ensure a higher level of security than is regularly available. For example, scholars have recognized encryption technology and passwords as valid methods to increase one's expectation of privacy in various computer data.[150] Understanding these security measures is essential because extreme tension often emerges in this context between the interest of law enforcement in prosecuting criminals and an individual's interest in keeping his or her information private.

As stated above, the Fourth Amendment not only protects against unreasonable "searches," but also guards against unreasonable "seizures."[151] In *United States v. Jacobsen*,[152] the Supreme Court held that a seizure of property occurs when there is a "meaningful interference with an individual's possessory interest in that property."[153] Accordingly, the Supreme Court has held that the installation of a beeper in a container did not constitute a seizure because it did not interfere with the defendant's possessory interest in the container.[154] Similarly, in *Arizona v. Hicks*,[155] the Supreme Court held that copying the serial number on an item of equipment did not interfere with the owner's possessory interest, and thus was not a seizure.[156]

---

144. *See* Steve Warmbir, *Closing Loopholes for People Preying on Kids On-line*, CHI. DAILY HERALD, Aug. 9, 1999, at A1, *available in* 1999 WL 23265684.

145. *See id.*

146. The defendant was found guilty on the lesser charge of "possession of child pornography" and sentenced to probation and community service. *Id.*

147. *See* Sergent, *supra* note 5, at 1196.

148. *Id.* at 1195-96.

149. *Id.* at 1197.

150. *See* Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1603 (1997); *see also* Sergent, *supra* note 5, at 1199-1200.

151. *See* U.S. CONST. amend. IV.

152. 466 U.S. 109 (1984).

153. *Id.* at 113. Note that an arrest is generally viewed as a seizure of the person. *See* United States v. Watson, 423 U.S. 411, 428 (1976) (Powell, J., concurring).

154. *See* United States v. Karo, 468 U.S. 705, 712-13 (1984).

155. 480 U.S. 321 (1987).

156. *See id.* at 324-25. It must be noted, however, that the Court found that moving the equipment to view the serial number was a "search." *See id.*

Defining a "seizure" in cyberspace, however, is much more problematic particularly because the information contained therein is intangible.[157] The Supreme Court has provided some guidance in applying "seizure" analysis to intangible information in the context of the telephone conversation, which may be instructive in determining the appropriate approach to computer data. Citing *Katz*, the Court held that a wiretap constituted a "seizure" of a telephone conversation.[158] A unanimous Court has not agreed upon this conceptualization of a conversation,[159] and therefore questions regarding when a seizure actually occurs in such a context remain problematic.

It has been suggested that *Katz* and *Hicks* might be reconciled by focusing on what the possessory interest in the seized item actually is.[160] For example, the possessory interest in a conversation lies in controlling the dissemination and use of the conversation, while the possessory interest in a tangible item consists largely in the item's use.[161] Likewise, copying information from a document or tape recording a conversation interferes with control and thus interferes with possessory interest; but photographing a scene or copying a serial number from an object does not meaningfully interfere with possession.[162] Following this line of reasoning, a computer file is more analogous to a written document or oral conversation, because the value of the file lies in the information therein.[163] Therefore, copying a computer file interferes with the owner's possessory interest and should constitute a seizure under the Fourth Amendment.[164]

3. Farewell to the Warrant Requirement?

The general rule is that once a reasonable expectation of privacy exists, a warrant based on probable cause is generally necessary to effectuate a search or seizure. It has been suggested that indiscriminate searches and seizures may be undesirable for either or both of two reasons.[165] First, warrantless searches expose completely innocent people and their possessions to interferences by government when there is no good reason to do so.[166] Second, indiscriminate searches and seizures are conducted at the

157. *See* Sergent, *supra* note 5, at 1185. This author suggests that due to the intangible nature of computer data, authorities can make copies without any interference with an individual's access; therefore, it could be argued that no possessory interest is interfered with at all. *See id.*

158. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

159. *See* Berger v. New York, 388 U.S. 41 (1967). Justice Black dissenting stated that "[i]t simply requires an imaginative transformation of the English language to say that conversations can be searched and words seized." *Id.* at 78 (Black, J., dissenting). Justice Harlan also dissented, stating, "Just as some exercise of dominion, beyond mere perception, is necessary for the seizure of tangibles, so some use of the conversation beyond the initial listening process is required for the seizure of the spoken word." *Id.* at 98 (Harlan, J., dissenting).

160. *See* Sergent, *supra* note 5, at 1186.

161. *See id.*

162. *See id.*

163. *See id.*

164. *See id.*

165. *See generally* Amsterdam, *supra* note 126, at 411.

166. *See id.*

discretion of law enforcement, who may act "despotically and capriciously" in the exercise of their power to search and seize.[167]

In *Johnson v. United States*,[168] the Supreme Court discussed the importance of the search warrant:

> The point of the Fourth Amendment . . . is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.[169]

In other words, where a warrant has been issued by a neutral magistrate it acts as insurance that probable cause exists.[170]

Probable cause must exist for a valid warrant to be issued.[171] Probable cause requires that there be some reasonable ground for belief in certain alleged facts.[172] Furthermore, even when a warrant is not required, a showing of probable cause is generally necessary to ensure that a search or seizure was reasonable.[173]

It is important to recognize that the "warrant clause" of the Fourth Amendment contains a particularity requirement. Namely, the warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized."[174] The particularity requirement serves several broad policy goals. First, the particularity requirement makes "general searches . . . impossible and prevents the seizure of one thing under a warrant describing another."[175] Second, a valid warrant should be sufficiently definite so that the executing officer can identify the property sought with reasonable certainty.[176] Finally, the particularity requirement is intertwined with the requirement that there be probable cause to search.[177] "The nature of the property will often give some indication as to how detailed a description is necessary."[178]

---

167. *See id.*

168. 333 U.S. 10 (1948).

169. *Id.* at 13-14.

170. Of course, probable cause represents the threshold of proof that must be satisfied before the power to search and seize is legitimated. *See* U.S. CONST. amend. IV.

171. *See* LAFAVE & ISRAEL, *supra* note 95, § 3.3(a), at 138.

172. *See* BLACK'S LAW DICTIONARY 1201 (6th ed. 1990).

173. *See id.*

174. U.S. CONST. amend. IV.

175. Marron v. United States, 275 U.S. 192, 196 (1927).

176. *See* LAFAVE & ISRAEL, *supra* note 95, § 3.4, at 161 (discussing the unrealistic standard set forth in *Marron* that with the warrant "nothing is left to the discretion of the officer executing the warrant").

177. *See id.*

178. Wayne R. LaFave, *Search and Seizure, The Course of True Law Has Not Run Smooth*, 1966 U. ILL. L.F. 255, 268. In other words, some property may be described generally due to its very nature, "[b]ut if the items sought are of a kind generally found in various places, then there is a need to be more specific." *Id.*

As the composition of the Supreme Court has changed, however, so has the Court's interpretation of the warrant "requirement." Judicial decisions have vacillated "between imposing a categorical warrant requirement and looking to reasonableness alone."[179]

4. When a Warrant Is Not Required

Where one would normally have a reasonable expectation of privacy, there are certain situations that give rise to exceptions to the warrant requirement. In *Johnson*, the Court stated that "[t]here are exceptional circumstances in which, on balancing the need for effective law enforcement against the right of privacy, it may be contended that a magistrate's warrant for search may be dispensed with."[180] Several of these exceptions, such as searches incident to arrest,[181] searches necessary to protect life,[182] searches in hot pursuit,[183] searches under exigent circumstances,[184] and searches conducted at the U.S. border,[185] will rarely be applicable to investigations of communication in cyberspace. Three other exceptions are important in this context, however. In applying them to the computer media some interesting conceptual extensions are evident.

First, when valid consent to search has been given, it generally has been accepted that the search is reasonable even without a warrant or any articulable suspicion.[186] Provided that the consent was knowing, voluntary, and intelligent, there is no Fourth Amendment problem.[187] In cyberspace, the consent exception may be implicated in one of two ways. First, if a sender of data consents to a law enforcement agent's reading the communication, then no warrant is required.[188] Suppose that an Internet user is a member of a "closed" chat room (one requiring a password for access). Obviously, if the user gives the password to a police officer, he has relinquished any expectation of privacy in the information.[189] This will be the case even if the user was not aware of the officer's identity.[190] Once a person entrusts another with information, he assumes a risk that the other will be an undercover agent.[191] This scenario is problematic, in so far as other chat room participants may not know that the password was given to anyone outside the chat group. However, courts are unlikely to sympathize with an individual who places herself in such a predicament. Note also that

179. California v. Acevedo, 500 U.S. 565, 582 (1991).

180. Johnson v. United States, 333 U.S. 10, 14-15 (1948).

181. *See* United States v. Robinson, 414 U.S. 218, 234-36 (1973).

182. *See* Mincey v. Arizona, 437 U.S. 385, 392-93 (1978).

183. *See* Warden v. Hayden, 387 U.S. 294, 298-99 (1967).

184. *See* United States v. Arias, 923 F.2d 1387 (9th Cir. 1990), *cert. denied*, 502 U.S. 840 (1991).

185. *See* United States v. Ramsey, 431 U.S. 606, 619 (1977).

186. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 232-33 (1973) (holding that consent must be voluntary, which is determined by looking at the totality of the circumstances); *see also* Sergent, *supra* note 5, at 1214-16 (discussing consent searches on "multiple-user computer systems").

187. *See Schneckloth*, 412 U.S. at 232.

188. *See* LAFAVE & ISRAEL, *supra* note 95, § 3.10, at 238.

189. *See Keeping Secrets*, *supra* note 150, at 1600.

190. *See id.*

191. *See id.*

the Fourth Amendment does not preclude an officer from misrepresenting his identity.[192]

Second, when the information has been disclosed to a third party with common authority over it, consent by the third party is valid.[193] According to *United States v. Matlock*,[194] the authority of the third party to consent is based on "mutual use of the property by persons generally having joint access or control for most purposes."[195] In *Matlock* the Court emphasized two requirements which would point towards "common authority": (1) that the consenting party could permit the inspection "in his own right," and (2) that the defendant had "assumed the risk" that the co-user would permit a search.[196] One scholar has suggested that whether or not a system manager of a multiuser computer network has the ability to consent to a search of files of its various users should depend on how the rights of access and control are allocated between the users and the systems manager.[197]

Third, when the information is in plain view of outsiders, it is "not protected because no intention" to keep it private has been exhibited; therefore, there has been no search.[198] Because the Internet is freely accessible to almost anyone, to expect privacy of information easily observable by the browsing public would be ridiculous. Furthermore, to assert that law enforcement officers have less right to travel the Internet is untenable. For these reasons, communications in cyberspace that are open to the public should be treated under the "plain view" exception. Of course, the plain view exception to a search does not necessarily mean that Fourth Amendment protection against unreasonable seizures would be excused as well. The Supreme Court has said that the plain view doctrine "authorizes seizure of illegal or evidentiary items visible to a police officer" if his "access to the object" has a Fourth Amendment justification.[199]

It is important to recognize that the law as it applies to computer technology is still in its infancy. Thus, it may be difficult to determine how the exceptions to the warrant requirement will ultimately be applied. Whether courts will extend existing exceptions or create new ones depends largely on policy. Perhaps the *Johnson* Court's statement about "exceptional circumstances" could be viewed as a benchmark. For example, if a warrant were required in all cases, the law enforcement system might be overburdened or the warrant process could be transformed into a mechanistic routine, sabotaging efforts to both protect privacy and combat crime. This premise supports the conclusion that the warrant should be used on a selective basis to "prevent those police practices that would be most destructive of Fourth Amendment values."[200]

---

192. *See id.*
193. *See* LAFAVE & ISRAEL, *supra* note 95, § 3.10, at 239.
194. 415 U.S. 164 (1974).
195. *Id.* at 171 n.7.
196. *Id.*
197. *See* Sergent, *supra* note 5, at 1214.
198. LAFAVE & ISRAEL, *supra* note 95, § 3.2, at 127.
199. Illinois v. Andreas, 463 U.S. 765, 771 (1983).
200. Sergent, *supra* note 5, at 1208.

V. Tenth Circuit Faces the Problem

The Tenth Circuit has on several occasions faced the problem of child pornography and the Internet. The court has addressed a statutory challenge as well as several constitutional attacks charging violations of the Fourth Amendment. While the current body of case law dealing with these issues is limited, it is important to understand the methods employed by the Tenth Circuit, as the future is sure to see more of such cases. Furthermore, the treatment of the Internet in the context of child pornography will undoubtedly shed light on the manner in which the Tenth Circuit will handle other cyber issues.

A. Statutory Interpretation

In a relatively recent case, the Tenth Circuit dealt with a challenge to a conviction under the CPPA. In *United States v. Wilson*,[201] the defendant appealed his conviction under the Act claiming that the jurisdictional element had not been met in his case.[202] More precisely, the defendant charged that the prosecution failed to prove the statutory requirement that the "visual depictions were produced using materials that had been . . . transported in interstate or foreign commerce."[203]

In *Wilson*, the court took the opportunity to define the meaning of "materials" found in the statute. The court chose to adopt a broad definition of the term holding that "materials" are not confined to the "ingredients" of the visual depiction, but include objects that are determined to give form or shape to the visual depictions.[204] In applying this definition to the defendant's case, the court found that indeed the requirement had not been met.[205]

In *Wilson*, the defendant was convicted by a jury based on evidence contained on ten computer diskettes. While the court agreed that the diskettes did travel in interstate commerce (at least from the manufacturer to the defendant's home state), there was a striking dissatisfaction with the case presented by the prosecution at the lower court. The court noted that the prosecution failed on several points. First, the prosecution

---

201. 182 F.3d 737 (10th Cir. 1999).

202. *See id.* at 740. Defendant was charged with violating 18 U.S.C. § 2252(a)(4)(B), which states that

> [a]ny person who knowingly possesses 3 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction . . . which was produced using materials which have been mailed or . . . shipped or transported [in interstate or foreign commerce], by any means including by computer, if — (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct; shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2252(a)(4)(B) (Supp. 1999).

203. *Wilson*, 182 F.3d at 740.

204. *See id.* (citing United States v. Bausch, 140 F.3d 739 (8th Cir. 1998), where the defendant was convicted under the same statute for taking pictures of two minor girls and the court found that the camera which the defendant used was from Japan which satisfied the "materials" requirement because it was shipped in foreign commerce).

205. *See id.* at 743.

failed to show that the diskettes were actually used to produce the graphic files.[206] Second, while some of the images originated out of state and it was likely that the defendant used his computer to download them, only one diskette out of the ten contained such images and three or more were necessary under the statute.[207] Finally, there was other evidence that some of the images were from German magazines, but no explanation was provided as to how those images found their way on to the diskettes in the defendant's possession.[208]

The *Wilson* decision illustrates the approach likely to be taken by the Tenth Circuit when faced with the task of defining statutory language in this context. The court took a very broad approach in its interpretation of "materials." Had it not been for the failure of the prosecution to link the diskettes, or the files on them, to interstate commerce, the court would have likely upheld the defendant's conviction.

B. Fourth Amendment Analysis in the Tenth Circuit

In *United States v. Carey*,[209] the Tenth Circuit dealt with several Fourth Amendment issues in the context of child pornography stored as computer data. In *Carey*, the defendant was charged with possession of a computer hard drive that contained one or more images of child pornography produced with materials shipped in interstate commerce.[210] The defendant appealed an order of the district court denying his motion to suppress material seized from his computer, arguing that it was taken as a result of a general, warrantless search. The *Carey* court agreed with the defendant and reversed.

In *Carey*, the defendant was under investigation on unrelated drug charges for some time prior to his arrest on child pornography charges. During the course of an arrest at the defendant's residence, officers elicited verbal consent to search the defendant's apartment and later received formal written consent.[211] During the course of the search, the officers found drug evidence as well as two computers that they believed would contain evidence of drug dealing.

After taking the computers to the police station, the officers obtained a warrant permitting them to search for evidence of the sale and distribution of controlled substances. During the search, a number of graphic files with sexually suggestive titles were downloaded. The detective conducting the computer search began to view the files and discovered child pornography. Ultimately, two hundred and forty-four such files were downloaded and transferred to nineteen disks.

---

206. *See id.* at 742.

207. *See id.* at 744.

208. *See id.*

209. 172 F.3d 1268 (10th Cir. 1999).

210. *See id.* at 1270. Defendant was charged under 18 U.S.C. § 2252A(a)(5)(B) (Supp. 1999). *See Carey*, 172 F.3d at 1270.

211. Defendant's written consent authorized "a complete search of the premises and property located at 3225 Canterbury #10, Manhattan, KS 66503" and stated, "I do freely and voluntarily consent and agree that any property under my control . . . may be removed by the officers . . . if said property shall be essential in the proof of the commission of any crime in violation of the laws of the United States." *Carey*, 172 F.3d at 1270.

The government analogized the computer search to looking for documents in a file cabinet, pursuant to a valid warrant, yet turning up child pornography.[212] They argued that seizure of the images was permissible because a valid warrant was obtained authorizing the search of any file that might contain evidence of drug crimes, and because the images were in plain view.[213] Furthermore, the government maintained that the defendant's consent to search his apartment extended to the search of all files on both computers found within it.[214]

The court rejected the government's arguments, finding that the files seized were not authorized by the warrant and that the scope of the defendant's consent to search his apartment did not permit the opening of files found on the computers. First, in addressing the warrant, the court stated that it allowed only the search of documentary evidence pertaining to the sale of narcotics.[215] Furthermore, the contents of the files were not covered by the "plain view" exception to the warrant requirement because the contents could not be seen without first opening the files.[216] The court stated that after viewing the first graphic file, the investigating officer was then armed with probable cause that the other files would contain similar depictions and should have sought a warrant.[217]

Next, the court in *Carey* addressed the scope of the defendant's consent, finding that it did not extend to the content of the graphic files.[218] The court noted that the officers were aware of this because a proper warrant to search for drug related evidence was obtained prior to any computer files being opened.[219] Since the files in question were labeled as graphic in nature and contained sexually suggestive titles, after opening the first one, the officer had reason to know what the others would contain.[220]

The opinion of the *Carey* court is important in several respects. First, the court's decision focused intensely on established Fourth Amendment standards and refused to condone the type of general searches against which those standards are designed to protect. Second, the court's analysis serves as a guide to both officers and prosecutors regarding what will be expected of them in the future. This is significant due to the fact that the law as it relates to computer technology is constantly evolving and those attempting to combat crime should know what will be required of them constitutionally.

Finally, the court in *Carey* addressed the analogy set forth by the government — that images stored in a computer may be likened to files in a file cabinet. The court recognized that this conception of computer files may be inadequate, and even warns that analogies like this may lead courts to "oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."[221]

---

212. *See id.* at 1272.
213. *See id.*
214. *See id.*
215. *See id.* at 1272-73.
216. *See id.* at 1273.
217. *See id.*
218. *See id.* at 1274.
219. *See id.*
220. *See id.*
221. *Id.* at 1275 (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data,*

This observation by the Tenth Circuit exhibits the quality of judicial restraint and understanding that is so essential as society moves onto the Internet and increases its computer usage.

In *United States v. Simpson*,[222] a case decided prior to *Carey*, the Tenth Circuit was again faced with Fourth Amendment challenges to a conviction for receiving child pornography; this time, in violation of 18 U.S.C. § 2252(a)(2).[223] The conviction was based on images stored on computer files, which belonged to the defendant and which were recovered by authorities during the execution of a search warrant.[224] On appeal, the defendant raised several Fourth Amendment arguments: (1) "that the search warrant was improperly obtained and executed," (2) "that the court admitted improper evidence and testimony," and (3) "that the evidence was insufficient to support a conviction."[225] A review of the case highlights how the Tenth Circuit applied the Fourth Amendment doctrines described above.

In *Simpson*, the defendant argued that certain evidence seized at his home and used to convict him should have been suppressed.[226] First, Simpson claimed that the search warrant was invalid because the facts presented to the issuing judge were insufficient to allow the judge to conclude that the evidence sought met the definition of child pornography[227] under Oklahoma law.[228] The affidavit presented to the issuing judge generally described the material being sought as "child pornography" and contained a statement by the affiant that he had received information from FBI agents regarding a deal struck with the defendant over the Internet to swap pornographic materials.[229] The court found that the information was sufficient to create probable cause justifying the issuance of the warrant.[230]

---

8 HARV. J.L. & TECH. 75, 104 (1994)). The court noted that "electronic storage is likely to contain a greater quantity and variety of information than any previous storage method" and that "computers make tempting targets in searches for incriminating information." *Id.*

222. 152 F.3d 1241 (10th Cir. 1998).

223. 18 U.S.C. § 2252(a)(2) provides:

> (a) Any person who —
>
> (2) knowingly receives, or distributes, any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution in interstate or foreign commerce by any means including by computer or through the mails, if —
>
> (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> (B) such visual depiction is of such conduct.

18 U.S.C. § 2252(a)(2) (Supp. IV 1999).

224. *See Simpson*, 152 F.3d at 1244.

225. *Id.*

226. *See id.* at 1246.

227. Child pornography is defined under Oklahoma law by 21 OKLA. STAT. § 1021.2 (Supp. 1999).

228. *See Simpson*, 152 F.3d at 1246. In addressing this claim, the court declares that the sufficiency of probable cause is determined by looking at the "totality of the circumstances" and deciding if "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id.* (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

229. *See id.*

230. *See id.* at 1246-47.

Simpson also contended that there was insufficient evidence to support probable cause to believe he actually possessed any illegal materials.[231] The court found that even though the transaction between the FBI agent and the defendant never took place (because Simpson was fearful of sending pornographic materials through the mail), the agreement between the parties made over the Internet provided sufficient evidence to conclude that the defendant possessed illegal materials.[232] The court rejected the defendant's emphasis on the fact that the agreement occurred anonymously over the Internet because the defendant gave the agent his real name and address.[233]

It is easy to accept that probable cause existed in the *Simpson* case mainly because of the fact that the appellant was ultimately found to have pornographic images of children stored in his computer files. However, a more thorough review of the facts of the case raises significant doubts as to whether probable cause existed. It is striking that the court admitted that the government's evidence was "almost entirely circumstantial."[234] In essence, the affidavit for the search warrant in the case was built around very little: a conversation in a chat room called "Kidsexpics" between an undercover agent and an individual who said that his name was "B. Simpson" and admitted to having child pornography, a proposed agreement to swap child pornography, and a series of e-mail messages which culminated in the appellant backing out of the agreement to trade.[235] These were *all* of the facts presented. There were no actual pornographic images presented and no one could vouch for the fact that they actually existed. Furthermore, that the appellant was the individual who engaged in the conversation with the undercover agent in the chat room was not certain. Any person could have used the appellant's e-mail address to send and receive messages.

In *Simpson*, the appellant analogized his computer disks and hard drive to "closed containers."[236] He argued that the government should be required to get a search warrant specifically authorizing their search.[237] The court rejected this analogy because there was no authority supporting it.[238] The *Simpson* court's rejection of the defendant's proposed analogy of computer disks and hard drive to closed containers is comforting in a sense. The decision is in line with the Tenth Circuit's later opinion in *Carey*. Hopefully, the hesitation in accepting analogies to more conventional media is a signal that the Tenth Circuit is willing to engage itself in an examination of the true nature of computer data.

VI. Privacy Concerns — Fourth Amendment Analysis May Yet Prove Sufficient

As noted in the introduction to this comment, the choices we make as a society with respect to the treatment of Internet searches under the Fourth Amendment will

231. *See id.* at 1247.
232. *See id.*
233. *See id.*
234. *Id.* at 1244.
235. *See id.*
236. *See id.* at 1248.
237. *See id.*
238. *See id.*

inevitably affect other areas of life. For this reason, courts should not rule blindly without regard to the way their decisions impact future generations. The law should continue to act within carefully circumscribed limits to ensure that the quality of freedom in our democratic society does not suffer unnecessarily in the name of "fighting crime."

Globally, the concern over online security and privacy is central to public discourse about Internet related issues. In the United States, the privacy debate is not new. However, technology increasingly enables and enhances the ability to gather, store, compile, search for and sort personal data. Over two hundred years ago, the founders of our Constitution declared that privacy was "the right to be let alone."[239] Since then, the Supreme Court has identified privacy rights arising from different parts of the Constitution. But, to date, no high court rulings definitively and directly apply to the complex privacy issues that are raised every time individuals log on to their computers.

Several commentators have questioned whether new privacy laws need to be enacted to deal with the online environment, or whether privacy rights should be more universally protected.[240] The debate is becoming more heated as Congress considers enacting legislation that would limit the use of encryption technology to further the goals of law enforcement.[241] This factor is troubling particularly because there are no clear answers. Obviously, crime control is a legitimate government interest, but how much privacy are we, as a society, willing to give up?

One commentator makes a philosophical argument regarding the degree of autonomy that we, as individuals, desire to maintain.[242] This idea is very important on a practical level as well because the way in which the issues are addressed will influence the degree of power that is handed over to law enforcement. The public discourse surrounding how much of *ourselves* we are willing to expose will likely become a more important political issue in the years ahead. Additionally, the courts will need to make a balanced response to the issue in hearing the cases.

As one author notes, an individual's ability to limit the flow of personal information has long been viewed as an essential step towards securing a healthy relationship with the outside world.[243] Continuing this, the author argues that privacy should be defined as selective control of access to information about herself or the group to which she belongs.[244] With this power over information, an individual can dictate to some degree how others viewed her, and how she wishes to interact with the world.[245] The diminished level of control over personal information that an individual experiences

239. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (recognizing the conditions the constitutional drafters deemed "favorable to the pursuit of happiness").

240. *See* Nicholas W. Allard, *Privacy On-Line: Washington Report*, 20 HASTINGS COMM. & ENT. L.J. 511, 526 (1998).

241. *See* Weinberg, *supra* note 68, at 681.

242. *See* Adler, *supra* note 93, at 1119.

243. *See id.*

244. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

245. *See* J.M. Balkin, *What is Postmodern Constitutionalism?*, 90 MICH. L. REV. 1966, 1988 (1992) ("Our ability to provide or withhold aspects of our private selves preserves and constitutes our autonomy.").

when she is outside the home or office should be balanced by the existence of a "private enclave where [s]he may lead a private life."[246]

There are a striking number of federal and state statutes that apply to aspects of electronic communication and information technology. Statutes thus deal with the interception and disclosure of electronic communications,[247] the protection of government maintained databases,[248] regulation of credit and financial reports,[249] and telemarketing,[250] to highlight just a few. However, many commentators conclude that there are few effective safeguards that protect personal data online, that there are gaping holes in existing laws, and that many existing laws are inconsistent, if not contradictory.[251]

Furthermore, the possibility of developing the Internet-wide search technology discussed *supra*[252] is very real indeed and raises numerous concerns beyond the scope of this comment. Clearly, however, such action by the government would constitute unprecedented intrusion into the private lives of individuals. While traditional Fourth Amendment analysis has yet to prove itself a perfect fit to current and future problems involving the Internet and electronic data in general, it is the best that we have.

By supporting Fourth Amendment protections, both government and individuals are ensured the healthy pursuit of their interests, which at times may conflict. Government should not be permitted an unqualified entrance; individuals' lives should remain their own.

VII. Conclusion: Moving Towards a Healthy Future Under the Existing Fourth Amendment Model

Thomas Paine warned that the "avidity to punish is always dangerous to liberty" because it pushes a nation "to stretch, to misinterpret, and to misapply even the best of laws."[253] Paine's concern is very real. There is a threat to liberty when legal principles, which are outdated or ill-fitted to deal with a particular problem, are applied by force. This comment uses the problem of child pornography on the Internet to illustrate the difficulties in applying existing Fourth Amendment analysis to Internet communications generally. This comment focuses on child pornography precisely

246. Tehan v. United States *ex rel.* Shott, 382 U.S. 406, 414 n.12 (1966) (quoting United States v. Grunewald, 233 F.2d 556, 581-82 (2d Cir. 1956)).

247. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1860 (codified as amended in scattered sections of 18 U.S.C.).

248. *See* Privacy Act of 1974, Pub. L. No. 93-579, 89 Stat. 1057 (codified as amended in scattered sections of 5 U.S.C.).

249. *See* Fair Credit Reporting Act of 1970, Pub. L. No. 90-321, 84 Stat. 1128 (codified as amended in scattered sections of 15 U.S.C.); *see also* Financial Institutions Regulatory & Interest Rate Control Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (codified as amended in scattered sections of 12.U.S.C.).

250. *See* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2395 (codified as amended in scattered sections of 47 U.S.C.).

251. *See* Robert O'Harrow Jr., *Laws on the Use of Personal Data Form a Quilt With Many Holes*, WASH. POST, Mar. 9, 1998, at A12.

252. *See supra* text accompanying note 106.

253. Paine, *supra* note 1, at 588.

because there is virtually universal dedication to the task of apprehending and convicting individuals who trade in child pornography. In other words, it should be an easy case. However, the case is not so easy, in the sense that we are still required to look at the implications of applying existing Fourth Amendment models to a situation with which it appears at times to be struggling to adapt.

As illustrated *supra*, the "expectations test" is an imperfect mechanism with which to deal with many of the new Fourth Amendment issues. First, one's subjective expectation of privacy in Internet communications will depend on the amount of technical knowledge that one possesses about the Internet in general, and is thus rendered somewhat meaningless. Who is the "average Internet user"? Does he or she know about encryption technology? Do they use it? Does the average Internet user know which types of computer data are more vulnerable to being uncovered? These questions are difficult to answer.

Second, the "objective" prong of the test, or what society is willing to recognize as "private," suffers the same fate. What does society want the limits on government action to be? Should this determination be left up to the courts who appear to be struggling to find an analogy buried in precedent?

In the interest of forwarding democratic ideals, it is essential that the courts carefully adapt this model to current problems. Judges and lawyers alike must be sensitive to the implications of all decisions made. They must strive to interpret the laws with liberty and justice as their highest goals. While fighting crime is important, it is not so important that the law should cease to develop concomitant to society.

The words of Justice Brandeis are worth reflecting on for their timeliness as well as their success in expressing the sense of immediacy with which the issues discussed in this comment should be addressed by those in the legal community:

> Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example . . . . To declare that in the administration of the criminal law the end justifies the means — to declare that the government may commit crimes in order to secure the conviction of a private criminal — would bring terrible retribution.[254]

Amy E. Wells

254. Olmstead v. United States, 277 U.S. 438, 468 (1928) (Brandeis, J., dissenting).