Washington and Lee Law Review

Volume 57 | Issue 1 Article 6

Winter 1-1-2000

# Computer Network Trespasses: Solving New Problems with Old Solutions

Susan M. Ballantine

# Computer Network Trespasses: Solving New Problems with Old Solutions

Susan M. Ballantine*

*Table of Contents*

I. Introduction ..... 210
II. Technical Background ..... 213
A. Development of the Internet ..... 214
B. Accessing and Using the Internet ..... 217
C. Summary ..... 220
III. Judicial and Scholarly Opinions on Internet Regulation ..... 221
A. Case Law ..... 221
1. The Lower Courts and the Internet ..... 221
2. The Supreme Court and the Internet ..... 225
B. Commentators' Views ..... 229
IV. Commercial ISPs, E-Mail, and Spam ..... 231
A. The Problem of Spam ..... 231
B. Trespass to Chattels May Provide a Theory to Combat Spam ..... 233
C. Early Application of Trespass to Chattels to Computer Technology ..... 235
D. Application of Trespass to Chattels to E-Mail and ISPs: *CompuServe, Inc. v. Cyber Promotions, Inc.* ..... 238
V. Protecting Private Network Providers from Unwanted E-Mail ..... 242
A. Factual Background of *Intel v. Hamidi* ..... 243
B. Intel's Arguments: How Trespass to Chattels Fails to Protect the Private Network Provider's Interests ..... 245
C. A Possible Solution for Private Network Providers ..... 249
VI. Conclusion ..... 255

* The author wishes to thank Professor Maureen Cavanaugh and Russell Jessee for their time and editorial assistance. The author also wishes to thank her parents, John and Beverley Ballantine, for their unfailing support. Finally, the author would like to thank Thomas Molony, Christy Ames, and Allison Pierce for their friendship and encouragement.

## I. Introduction

Ours is the information age.[1] No longer do we strive for power through production. Instead, we garner economic advantage through the information we control and disseminate.[2] Technology has made this paradigm shift possible.[3] However, with change come problems. For example, electronic mail (e-mail)[4] has begun to create unexpected difficulties for private network providers.[5] The primary question has become who may control the informational content on a network and how they may do so. In other words, we must ask whether and how the law can protect the private network providers' interest in restricting access to the flow of information on its network.

One corporation's attempt to control the information flowing to its network from outside sources has given rise to a legal battle.[6] In December 1996, employees of computer chip giant Intel Corporation (Intel)[7] received e-mail from a group named FACE Intel.[8] FACE Intel, founded by Ken Hamidi, is a group of

---

1. *See* ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 1-8 (1994) (discussing development of economic base in information and growing recognition of need to answer what it means to be in information age); Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1162-63 (1997) (stating that society has entered information age as result of transformation of economic base from industry to information).

2. *See* BRANSCOMB, *supra* note 1, at 3-4 (stating that transactions in information occur whenever someone believes he or she will profit from sale of such information); *see also* John O. McGinnis, *The Once and Future Property-Based Vision of the First Amendment*, 63 U. CHI. L. REV. 49, 102 (1996) (referencing value of information and growth of Internet); Michael I. Meyerson, *Virtual Constitutions: The Creation of Rules for Governing Private Networks*, 8 HARV. J.L. & TECH. 129, 149 (1994) (observing that private information has economic value).

3. *See* BRANSCOMB, *supra* note 1, at 3 (stating that explosion in information trafficking has resulted from technological revolutions that make gathering, organizing, and transmitting information faster and easier).

4. *See* Wendy R. Leibowitz, *E-mail Abuses Abound*, NAT'L L.J., Jan. 11, 1999, at 10, 10 (commenting that e-mail will be most ubiquitous source of trouble for business owners).

5. In this Note, the term "private network provider(s)" refers to private entities such as employers and some universities. To refer to companies whose business is providing Internet connection services, this Note uses the term "Internet service provider" or ISP.

6. Please note that all sources related to case documentation in *Intel v. Hamidi* are available at *Intel v. Hamidi* (visited Jan. 14, 2000) <http://www.Intelhamidi.com/casedocuments.htm>.

7. *See* Walter Isaacson, *Man of the Year: The Microchip Is the Dynamo of a New Economy . . . Driven by the Passion of Intel's Andrew Grove*, TIME, Dec. 29, 1997, at 52, 52 (explaining that Intel is private company that produces nearly 90% of world's microprocessors).

8. *See* Intel's Memorandum of Points and Authorities for Intel's Motion for Summary Judgment at 1, Intel Corp. v. Hamidi, No. 98AS05067 (Sacramento Super. Ct. filed Dec. 9, 1998) [hereinafter Intel's Motion for Summary Judgment] (explaining that Intel had received large number of e-mail from FACE Intel), *available at* <http://www.Intelhamidi.com/summaryjudgment.htm>; *see also FACE Intel* (visited Jan. 14, 2000) <http://www.faceintel.

former Intel employees who have banded together for the purpose of protesting Intel's personnel policies.[9] FACE Intel spreads its message of opposition by maintaining a World Wide Web (Web) site and, formerly, by sending unsolicited bulk e-mail to current Intel employees.[10] Intel has not challenged the existence of the Web site, but it did decide it would no longer tolerate the e-mail that FACE Intel and Hamidi were sending over the Intel computer network.[11]

In early 1998, a wave of e-mail from FACE Intel caught Intel's attention.[12] Intel responded by asking Hamidi and FACE Intel to cease and desist from sending any additional e-mail over the Intel computer network, including the company e-mail system.[13] Despite Intel's demand, Hamidi sent another bulk e-mail in September 1998.[14]

Hamidi's refusal to comply with Intel's request ultimately led Intel to file a complaint, based on trespass to chattels and nuisance theories, in Sacramento, California Superior Court in early October 1998.[15] Intel named both Hamidi and FACE Intel as defendants.[16] The superior court responded favorably to Intel's complaint and issued a preliminary injunction that prohibited Hamidi from sending any further e-mail to Intel employees over Intel's computer network.[17] In June 1999, the court granted summary judgment and made the temporary injunction permanent.[18]

---

com/whoweare.htm> (explaining acronym, purpose of group, and setting forth FACE Intel's grievances against company)

9. *See FACE Intel* (visited Jan. 14, 2000) <http://www.faceintel.com> (explaining FACE Intel's purpose); *see also* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (stating FACE Intel's purpose). Intel has sued for an injunction against Hamidi personally as well as against FACE Intel as a group. Complaint, Intel Corp. v. Hamidi, No. 98AS05067 (Sacramento Super. Ct. filed Oct. 6, 1998) [hereinafter Complaint], *available at* <http://www.Intelhamidi.com/intellawsuit.htm>.

10. Intel's Motion for Summary Judgment, *supra* note 8, at 1.

11. *See generally* Complaint, *supra* note 9 (seeking to enjoin Hamidi's use of Intel computer network to send e-mail to Intel employees).

12. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (explaining when Intel decided to take action in response to Hamidi's e-mail).

13. *Id.* at 2.

14. *Id.* at 1.

15. *See* Complaint, *supra* note 9, at ¶¶ 4-12, 14-15 (stating that Intel seeks recovery under trespass to chattels and nuisance theories).

16. *See id.* (naming Hamidi and FACE Intel as defendants).

17. *See* Preliminary Injunction, Intel Corp. v. Hamidi, No. 98AS05067 (Sacramento Super. Ct. issued Nov. 24, 1998) [hereinafter Preliminary Injunction] (granting preliminary injunction until final judgment after trial on merits), *available at* <http://www.intelhamidi.com/injunctionproposal.htm>.

18. *See* Order for Entry of Final Judgment, Intel Corp. v. Hamidi, No. 98AS05067 (Sacramento Super Ct. June 16, 1999) (stating that court issued injunction in favor of Intel on June 16, 1999), *available at* <http://www.intelhamidi.com/permanentinjunction.htm>.

As a private company, Intel uses its private e-mail system and computer network to provide its employees with e-mail and Internet access, but it does not provide Internet access to any outside parties.[19] Through its lawsuit against Hamidi, Intel sought to protect its interests in its proprietary e-mail system and computer network.[20] To persuade the court to protect Intel's interests, Intel argued that intrusions into its proprietary computer system constitute a trespass to chattels under California law.[21] Intel based its theory on cases in which Internet service providers (ISPs) have successfully argued that unsolicited bulk e-mail constitutes a trespass to chattels, namely the ISPs' computer networks.[22]

This Note argues that it is incorrect to apply the trespass to chattels theory to cases in which private network providers, specifically employers, seek to protect their interests in their computer networks.[23] Trespass to chattels requires that a plaintiff demonstrate tangible harm.[24] It is more difficult for private network providers than for ISPs to meet this requirement.[25] This Note proposes that analogizing trespasses to a private network and trespass to land provides more adequate protection to the private network provider's interest in controlling the information and activities on the provider's network.[26] In trespass to real property, the plaintiff must show only that the defendant was on the plaintiff's property without permission. Under the standard proposed in this Note, the plaintiff private network provider could prevail by showing that the defendant had continued to send e-mail to the plaintiff's network despite notice that the defendant no longer had permission to do so. This standard would allow the provider to protect its network without needing to

---

19. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 3 (stating that Intel's e-mail system is for Intel corporate use only and stating that Intel has written policies for employee use of e-mail system). Intel's policy states that employees may use the network for business and for limited personal purposes. *See id.*

20. *See* Complaint, *supra* note 9, at ¶¶ 6, 9-10 (stating that Intel is protecting private computer network).

21. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 3 (describing Intel's trespass to chattels argument).

22. *See infra* Part IV (discussing development of trespass to chattels as applied to electronic trespasses and ISPs). *See generally* America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998) (finding that advertiser's unsolicited bulk e-mail to ISP's customers over ISP's network constituted trespass to chattels); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (same).

23. *See infra* Part V.B-C (arguing that trespass to chattels does not adequately protect private network provider's interest in controlling information flowing to its network).

24. RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965); *see also infra* Part IV.B (setting forth requirements for trespass to chattels).

25. *See infra* Part V.B (comparing trespass to chattels in cases involving ISPs and private network providers).

26. *See infra* Part V.C (arguing that trespass to real property analogy will provide greater protection to interests of private network provider).

show tangible harm but would limit the relief to those instances in which the defendant had actual notice that it no longer had the privilege of sending e-mail on the private provider's network.

Part II of this Note provides the technical background necessary for understanding the analysis. First, Part II.A briefly describes the Internet's development.[27] Parts II.B and II.C then differentiate between the Web and e-mail as discrete subsets of Internet communication.[28] To provide a paradigm for the analysis of e-mail issues, Part III discusses how the courts and the commentators thus far have approached broader Internet-related issues.[29] Part IV discusses attempts by commercial ISPs to control e-mail messages that advertisers send over the ISPs' networks using the trespass to chattels theory.[30] Part V.A of this Note fully develops the facts of the *Intel* case.[31] Part V.B analyzes why the trespass to chattels cause of action is not the appropriate theory for protecting private network providers' interests in their private property.[32] Part V.C concludes that analogizing trespasses to private networks and trespasses to land can better protect the interests of the private network provider.[33]

## *II. Technical Background*

The Internet provides a large number of people with access to an extremely varied supply of information.[34] Necessarily, the methods for using Internet resources and for communicating on the Internet are not all the same. For example, e-mail allows users to deliver specific information to specific recipients while the Web allows users to "post" information for other users to find according to their interests.[35] Distinguishing between communications

---

27. *See* Part II.A (describing development of Internet).

28. *See infra* Part II.B-C (discussing accessing Internet and modes of communication on Internet).

29. *See infra* Part III (discussing court and commentator approaches to Internet-related issues).

30. *See infra* Part IV (discussing current state of law with respect to ISPs' attempts to control unsolicited bulk e-mail from unauthorized sources).

31. *See infra* Part V.A (setting forth facts of *Intel* case).

32. *See infra* Part V.B (distinguishing *Intel* from ISP cases).

33. *See infra* Part V.C (arguing that real property notions will more adequately protect private network providers' interests).

34. *See* Bob Norberg, *Price Right for Web E-mail, but Ads Part of Deal*, THE PRESS DEMOCRAT, Sept. 7, 1998, at D1 (stating that one e-mail provider, Hotmail, has 22 million users and is growing at rate of 100,000 subscribers per day); *Global Internet Statistics*, (visited Jan. 14, 2000) <http://www.glreach.com/globstats/> (stating that approximately 243 million people world-wide have access to Internet today and that by end of year 2000 projected 327 million people will have access).

35. *See infra* Part II.C (describing ways to utilize information on Internet); *infra* note 66 (explaining publishing on Web pages).

on the Internet may help explain why an employer will have a greater interest in prohibiting or limiting e-mail that flows to and over its system, while at the same time the employer may have little or no concern for controlling the content of others' Web postings.[36]

### *A. Development of the Internet*

In simplest terms, the Internet is a "network of networks."[37] A basic network is a group of interconnected computers that exchange files and messages and that often share equipment such as printers.[38] The innumerable connections among smaller networks of linked computers create the giant network called the Internet.[39] Given the breadth of the Internet, its development is both complex and complicated. The Internet originated from projects in computer networking connecting multiple computers in order to share and to transmit information.[40] By the early 1980s, this growing network reliably

36. *See Developments in the Law – The Law of Cyberspace: Internet Regulation Through Architectural Modification: The Property Rule Structure of Code Solutions*, 112 HARV. L. REV. 1574, 1649-56 (1999) (discussing competing issues of access to material available on Internet and exclusion of access through copyright protection). The development note observes that the Internet has made otherwise protected materials freely available and thus compromised the promise of copyright. *Id.* at 1650. The note cautions that this availability may hamper the growth of the Internet as individuals limit what material they place on the Internet in their effort to protect their interest in their own product. *Id.*

37. *See* ACLU v. Reno, 929 F. Supp. 824, 830-49 (E.D. Pa. 1996) [hereinafter ACLU I] (explaining factual background of Internet and related available technologies). Pundits and commentators use a variety of metaphors to refer to the phenomenon know as the Internet. *See* Robert C. Cumbow, *Cyberspace Must Exceed Its Grasp, or What's a Metaphor? Tropes, Trips and Stumbles on the Info Highway*, 20 SEATTLE U. L. REV. 664, 667-68 (1997) (observing many different metaphors for Internet); Kent N. Schneider & Timothy P. Hedley, *The World Wide Web: A Promising Tool for Legal Research*, 52 J. MO. B. 301, 303 (1996) (describing web metaphor for Internet as apt). For an esoteric description of the "net" metaphor, see KEVIN KELLY, OUT OF CONTROL, 25-26 (1994).

38. *See ACLU I*, 929 F. Supp. at 830-31 (explaining computer networks).

39. *See id.* (explaining how links among multiple computer networks create Internet). Internal networks, or "intranets" also exist. Intranets are networks internal to an organization, and they do not provide access to the Internet. *Id.*

40. *See* DOUGLAS E. COMER, THE INTERNET BOOK 49-53 (1995) (explaining early developments in Internet technology). *See generally id.* (explaining Internet in lay person's terms). After researchers succeeded in connecting nearby computers through local area network (LAN) technology, they began efforts to expand connections in order to transfer, irrespective of distance, data among computers. *See id.* at 49-53 (discussing LAN technology and increasing availability of Wide Area Networks (WANs) to connect computers located long distances from one another and elaborating on desirability of single network that would permit data transfer and information access among local and long distance computers). Several private companies then formed a nonprofit company to build a new WAN across the nation in an effort to expand the growing network. *See id.* (explaining development of current Internet by private companies); *see also* Henry H. Perritt, Jr., *What Is The Internet?*, 443 PLI/PAT. 11, 13 (1996) (commenting

connected a limited number of research facilities and university academic facilities across the country and world.[41] The network known as the Internet came into existence and continues to function because numerous institutions, companies, and individuals have agreed and have chosen to utilize common software protocols for computer communication.[42]

Two developments in Internet software proved particularly important for connecting large numbers of computers across long distances: Internet Protocol (IP) software and Transmission Control Protocol (TCP) software. IP software provides the basic communication capacity without which a computer cannot use the Internet.[43] TCP software provides an organizational framework for the information that the IP software transmits.[44] The primary advantage of the TCP/IP design is that it accommodates differences in computers, networks, and available services which in turn allows large numbers of computers to communicate.[45] This flexibility in the TCP/IP software allows computer users to meet their own computing needs on a local level while also connecting to the information resources of the Internet.[46]

---

that funding for Internet has shifted from government subsidy to private funding). Perritt also makes the point that no single entity "owns" the Internet. *Id.*; *see ACLU I*, 929 F. Supp. at 831-32 (discussing administration and ownership of computers using Internet for communication).

41. *See* COMER, *supra* note 40, at 63 (stating that Internet worked reliably to interconnect academic and research facilities).

42. *See ACLU I*, 929 F. Supp. at 832 (stating that Internet exists and functions because various entities have independently decided to use same data transfer protocols).

43. *See* COMER, *supra* note 40, at 107-14 (explaining that Internet Protocol software is necessary for sending and receiving any information on Internet). The term "protocol" refers to the agreement to use a common computer language so that two computers can exchange information. *Id.* at 107.

44. *See id.* at 115-20 (explaining that TCP software makes reliable communication possible by ordering packets of information sent on Internet by IP software). TCP/IP software helped to resolve the problems that arose from the incompatibility among various computers and networks by providing a common application package that permits vastly different computers and computer networks to exchange information. *See id.* at 98 (explaining how TCP/IP software helps solve problem of incompatibility of networks and computers); *see also id.* at 86 (stating that Internet offers many services but that primary advantage of Internet is design of TCP/IP software that accommodates changes in computers, networks, and available services). By using the TCP/IP standards, very different computers can connect with each other, thus allowing large numbers of computer users to communicate. *See* Perritt, *supra* note 40, at 13-14 (discussing unique features of Internet as part of national information infrastructure). Perritt explains that the TCP/IP protocol permits computers that do not use the same hardware (for example, an IBM or Toshiba computer) or software (for example, Microsoft Windows or DOS) to transmit data between one another. *Id.*

45. *See* COMER, *supra* note 40, at 86 (explaining that TCP/IP software allows entities with different computers to communicate).

46. *See id.* (commenting upon difficulty of forcing all computer users to use same computer resources when each entity often has its own computing needs). However, given the recent charges against Microsoft that allege violation of the antitrust laws in the distribution of

Computer networking occurs when software programs in separate computers exchange information through a client-server relationship.[47] Current technology enables this networking for three reasons.[48] First, programs, not computers, communicate by using the common protocol software to exchange information.[49] Second, the TCP/IP software does not actually create or run application programs.[50] Rather, the protocol permits one program to call another, and communication occurs once the receiving program "answers."[51] Last, because computers can run more than one program at the same time, a single server can accommodate a large number of users virtually simultaneously.[52] For example, a single server can provide services for users within the network, as well as provide information to multiple users calling from outside a network.[53] Thus, networking of multiple computers and users becomes possible at a local level. Because of the flexibility of the software

---

its software, it is possible to argue that most computers already use the same software, regardless of an entity's individual computing needs. *See* United States v. Microsoft, Corp., 980 F. Supp. 537, 539-40 (D.D.C. 1997).

47. *See* COMER, *supra* note 40, at 123-24 (explaining that client-server relation permits diversity of services on Internet). Scientists use the term "distributed computing" to refer to this seemingly arbitrary phenomenon of interaction between computers of varying sizes and complexity. *Id.* at 122. In client-server relationships, the server computer offers programs and files that the client computer accesses. *Id.* 123-24. Communication then occurs between the server program and the client program. *Id.* at 124. Typically, individual users employ client programs to access information available through server programs. *Id.* The server, however, always must be ready to receive requests for information. *Id.* at 125. If the server's computer operating system fails, then anyone using the server program will lose connection. *Id.* As long as the server program continues to run, then it will continue to execute information delivery. *Id.* If the server program is not available, then the client software will get an error message and will be unable to communicate with the server. *Id.*

48. *See infra* notes 47-52 and accompanying text (explaining networking technology).

49. *See* COMER, *supra* note 40, at 123 (explaining that software, not computers, communicates). Comer explains that a common misstatement among Internet users is that their "computers have communicated." *Id.* He comments that while the distinction seems trivial, it is important to understanding how a single computer can engage in "multiple conversations with other computers." *Id.*

50. *See id.* (stating that transfer of data over Internet does not automatically start programs on receiving machine).

51. *See id.* (analogizing computer program interaction to telephone conversation in which communication only occurs if receiving computer program answers). A client computer's "call" does not trigger a response from the server; rather, computers only communicate when the server computer is already available to "answer" calls from the client computer. *Id.* If the server computer is not available to answer, then the software programs cannot communicate. *Id.*

52. *See id.* (stating that computers can run more than one program at same time). Computers can even run more than one copy of the same program at the same time. *Id.* at 124. This capacity permits the computer to serve a large number of users simultaneously. *Id.*

53. *See id.* By running multiple copies of the same program, server computers can seemingly run the same program for multiple users virtually simultaneously. *Id.*

protocols, the Internet can then provide diverse information and services for a large number of simultaneous users.[54]

### *B. Accessing and Using the Internet*

Individuals access the resources of and communicate over the Internet in two principal ways.[55] Networks connected to the Internet typically are available to computer users through employers, universities, or even public libraries.[56] Alternatively, individuals can access the Internet through a personal computer that is connected via modem to an ISP, such as CompuServe or America Online, that provides Internet access for a fee.[57] After connecting to the ISP's proprietary network, the user then can link to the Internet.[58] The ISP's proprietary network generally provides its own information and services to the subscribers in addition to access to the resources of the Internet.[59] These various options for connecting to the Internet have made the Internet and its resources available to an ever-increasing number of people.[60]

Once having accessed the Internet, an individual can research available sources and communicate with other users in a variety of ways.[61] Two of the

54. *See id.* at 122 (discussing effect of distributed computing on Internet, permitting many different types of services for Internet users). Comer also points out that the variety of available services results in a variety of ways to interact over the Internet. *Id.* at 122-25.

55. *See* ACLU I, 929 F. Supp. 824, 832-34 (E.D. Pa. 1996) (elaborating on different options for connecting to Internet). In addition to access from a home or work computer, one can connect to the Internet from computers located at schools, libraries, or storefront computer coffees shops. *Id.*

56. *See id.* (enumerating different types of networks that can provide Internet access).

57. *See id.* (stating that one can use modems in personal computers to access network that provides connection to Internet); *see also* Perritt, *supra* note 40, at 17 (stating that as number of users interested in Internet access has increased, so has interest in services providing Internet connections). Perritt states that there are thousands of companies that provide Internet access. *Id.* These ISPs can be local or national. National companies include America Online, CompuServe, Microsoft, and AT&T. *Id.* Some companies, such as AT&T and MCI, offer Internet connections in addition to their other services. *Id.* Individuals connect to the ISP through modem and phone line, and once connected to the ISP's network, the user can then gain access to the larger Internet. *Id.*

58. *See ACLU I*, 929 F. Supp. at 833 (stating that individuals can access ISP's proprietary computer network and utilize those resources and also thereby access resources of Internet).

59. *See id.* (stating that ISPs provide access to extensive content on own proprietary computer network in addition to access to Internet resources).

60. *See id.* at 832-34 (explaining that people can access Internet from variety of outlets, including home and work computers). Although because of the Internet's decentralized nature it is difficult to determine the number of people accessing the Internet, there is no doubt that the number is growing rapidly. *Id.* at 830-31. Experts estimated that Internet use would grow to over 200 million users by the year 1999. *Id.*

61. *See id.* at 834 (observing that there are many methods of communication available through Internet).

most well-known methods are remote information retrieval through the Web and one-to-one messaging via e-mail.[62] Each of these methods is a different medium through which users communicate at differing levels of interactivity.[63]

Information provided on Web pages can achieve remarkable dispersion;[64] however, the information on Web pages is available only to those who actively search for the information.[65] By using a common computer language, creators of Web pages make their information easily retrievable by anyone using the Internet.[66] To access the available information, Internet users formulate

62. *See id.* (listing most common methods of communications on Internet including e-mail, "list servs," USENET newsgroups, and real time "chat rooms"). Because technology changes rapidly, it is difficult to create a complete list at any given moment. *Id.*

63. *See* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123-24 (W.D. Pa. 1997) (differentiating among Web sites by describing sliding scale of interactivity between merely posting information and actively promoting and conducting business over Internet); *see also* CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1268 (6th Cir. 1996) (finding personal jurisdiction based on defendant's conducting business by electronic transmissions); Cumbow, *supra* note 37, at 667 (stating that Internet is not physical "space" but rather medium of communication). Cumbow argues, for example, that e-mail and the Web are not distinct locations on the Internet, but rather they are different ways of using the Internet. *Id.* at 667-68. Under personal jurisdiction analysis, a court must determine whether or not the defendant has sufficient minimum contacts with the forum. International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945); *see infra* notes 90-94 (discussing Internet related cases that address personal jurisdiction issue). *See generally* David D. Tyler, Note, *Personal Jurisdiction via E-mail: Has Personal Jurisdiction Changed in the Wake of* CompuServe, Inc. v. Patterson*?*, 51 ARK. L. REV. 429 (1998) (concluding that in assessing personal jurisdiction, courts will have to analyze electronic contacts, including e-mail, on case-by-case basis, but that e-mail can be basis of jurisdiction if it meets standards of personal jurisdiction inquiry).

64. *See* ACLU I, 929 F. Supp. 824, 836-38 (E.D. Pa. 1996) (explaining that Web's design makes information available to potentially very large audience); *see also* ACLU v. Reno, 521 U.S. 844, 870 (1997) [hereinafter ACLU II] (articulating appreciation for breadth of potential audience for information available on Web).

65. *See ACLU I*, 929 F. Supp. at 834-37 (discussing Web site information posting and its availability only to those who seek it).

66. *See id.* at 837-38 (stating that publishers must format information to common Web standards in order to publish information on Web using Web pages). In order to "publish" information on a Web page, or on a Web site, a user must have a computer connected to the Internet and that computer must run software that is "server software." *Id.*; *see supra* note 47 (explaining "server software"). Furthermore, the user must publish the material in "hypertext" markup language (HTML), which is the common language for all materials accessible over the Internet. *ACLU I*, 929 F. Supp. at 836. Publishing in HTML allows publishers to make their information available in a wide variety of "documents," from plain text to advanced graphics and animation. *Id.* The standardized formatting provides a common set of rules in order to allow information exchanges. *Id.* Although Web pages generally are accessible to all users, Web publishers do have the option to make their information accessible only to those with authorization. *Id.*; *see also* M. Ethan Katsh, *Rights, Camera, Action: Cyberspatial Settings and the First Amendment*, 104 YALE L.J. 1681, 1700-02 (1995) (explaining hypertext and its flexibility and attributes).

searches which they submit to search engines that run the search through many available Web pages.[67] The search engine then presents a list of Web pages that might contain the desired information.[68] Web browsers, software interfaces between a computer and the Internet, then allow the user to view, to retrieve, and to move among (browse) the search results.[69] To facilitate information retrieval, Web pages and documents often have links to other Web pages that contain related information.[70] Thus, by browsing the Web, computer users can access the mass of information available over the Internet.[71]

Another way to utilize the Internet is through e-mail, which, in its simplest application, involves sending a single message to a targeted audience rather than waiting for someone to access the information.[72] Thus, e-mail is similar to sending a letter, albeit without a thirty-three cent stamp.[73] However, e-mail is vastly more complex than a letter sent by regular mail because one instanta-

67. *See ACLU I*, 929 F. Supp. at 837 (explaining that numerous "search engines" facilitate finding information on Web). Search engines are services that routinely catalog the content of both the Internet and the Web and allow users to search for information using key words. *Id.*

68. *See id.* (explaining how search engines permit users to find information on Internet).

69. *See* Thomas A. Piraino, Jr., *An Antitrust Remedy or Monopoly Leveraging by Electronic Networks*, 93 NW. U. L. REV. 1, 4 n.19 (1998) (defining and explaining use of Web browsers); *see also* Daniel Kadlec, *AT&T Betting on Its Bundle*, TIME, Feb. 15, 1999, at 44, 47 (documenting how Web browsing is changing). Browsing the Web is changing as more Web sites become "portals." *See* Michael Krantz, *Star Wars*, TIME, Feb. 15, 1999, at 47. "Portals" are "supersites" from which a user can access search engines and direct links to shopping and news. *Id.*

70. *See* ACLU II, 521 U.S. 844, 852 (1997) (explaining that one document or Web page often has links to other related Web pages or documents). A link, or hyperlink, is highlighted text or graphics on a Web page that a user can select and that automatically sends the user to another Web page without having to type in a new address. *See* Bruce P. Keller, *Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property*, 11 HARV. J.L. & TECH. 401, 419 n.87 (1998) (explaining "links").

71. *See* ACLU I, 929 F. Supp. 824, 836 (E.D. Pa. 1996) (describing Web as one of several methods to communicate using Internet). The Web is but one way by which users of the Internet post and retrieve information. *Id.*

72. *See id.* at 834-37 (discussing one-to-one messaging and Web site information posting).

73. *See id.* at 834 (explaining that, in principle, sending e-mail message is similar to sending letter to single recipient, although e-mail does not go through central processing point to arrive at destination); *see also* Jan Hemm Pritchard, *E-mail Privacy: An Oxymoron?*, 53 J. MO. B. 239, 239 (1997) (stating that e-mail is different from regular letters because senders believe themselves to be anonymous and because language in e-mail tends to be more harsh and crude than in letters or face-to-face conversation); Kevin J. Baum, Comment, *E-mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1013 n.18 (1997) (listing commentators who have noted differences between e-mail and more traditional methods of communication). In Internet vernacular, people often refer to the United States Postal Service as "snail mail." *See* David J. Loundy, *E-Law 4: Computer Information Systems Law & System Operator Liability*, 21 SEATTLE U. L. REV. 1075, 1080 (1998) (explaining that regular e-mail users refer to U.S. or land-based mail as "snail mail").

neously can send a single message that includes not only text but also graphics, video, and sound.[74] E-mail permits users to send messages from their own network directly to targeted recipients across the globe who have e-mail addresses on any other network that also is linked to the Internet.[75] Using computer-run e-mail application software, a user composes a message from a computer on one network, and then the software sends the message across the Internet to the recipient's e-mail address on the same or another network.[76] The recipient's e-mail software then stores the recipient's e-mail in the recipient's personal mailbox, which is usually computer disk storage space on the network.[77] Of course, storage of large numbers of e-mail can result in an overload of the network's physical limits, causing the system to shut down.[78] Nevertheless, in general e-mail can be an easy and inexpensive way to send messages.

### *C. Summary*

The Internet provides a large number of people with access to an extremely varied supply of information.[79] Users access the Internet through affiliated institutions or through ISPs.[80] Internet users then use the Internet

---

74. *See* COMER, *supra* note 40, at 143 (listing services that e-mail systems provide to permit complex communication).

75. *See id.* at 152 (explaining that users can send e-mail to recipients on other networks by using Internet connection). For example, a subscriber of the CompuServe network can send e-mail to a subscriber of AOL's network. *Id.*

76. *See id.* at 144 (describing how individual users participate in e-mail exchanges using e-mail application software and Internet). A user can send e-mail to one or more addressees. *Id.* at 150.

77. *See id.* at 144 (explaining that each e-mail user has mailbox identified by unique number address and that computer network stores received e-mail on disk). When e-mail arrives at the mailbox address, the e-mail software application automatically stores the message in the user's mailbox. *Id.* Usually, only the actual user of the mailbox can access the content of the mailbox. *Id.* However, oftentimes employers may retain the right to examine the e-mail that employees send and receive. Scott A. Sundstrom, Note, *You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2064-67 (1998) (commenting upon frequency of e-mail monitoring in workplace).

78. *See* Gindin, *supra* note 1, at 1167-68 (stating that excessive amount of e-mail that online advertisers have sent can overload ISP systems and cause networks to shut down); John Simons, *The Battle over Spam Gets Ugly*, U.S. NEWS & WORLD REP., May 12, 1997, at 55 (commenting on shut-down of ISP after it received more e-mail than network could process); *see also infra* notes 137-44 and accompanying text (discussing costs of spam and excessive amount of e-mail).

79. *See supra* note 34 (discussing number of Internet users); *see also* Krantz, *supra* note 69, at 46-48 (presenting information on how accessing information over Internet is changing); *see also supra* note 69 (discussing changes in Web browsing).

80. *See supra* notes 53-58 and accompanying text (discussing how users can gain access to Internet).

either by browsing the Web or by communicating directly with other users through e-mail.[81] The Web allows an individual or an organization such as CNN to post information, hoping that another will then access the information.[82] In contrast, e-mail allows a user to send particular information to a specific targeted recipient: a friend, a consumer, or an interested party.[83] A user can opt to spread his or her message by e-mail, via a Web page, or by using both methods; choosing one option does not foreclose the other. Thus, although e-mail and the Web both are media through which a user may access the resources of the Internet, they differ markedly in how a user delivers, receives, or obtains information.[84]

## *III. Judicial and Scholarly Opinions on Internet Regulation*

### *A. Case Law*

#### *1. The Lower Courts and the Internet*

The Internet has become an interesting battleground for courts and for commentators.[85] Although the Internet has grown rapidly in a relatively short period of time, few courts confronted Internet issues before 1996.[86] The

81. *See supra* notes 59-76 and accompanying text (discussing how users communicate and use resources of Internet).

82. *See supra* notes 65-71 and accompanying text (discussing Web use).

83. *See supra* notes 72-77 and accompanying text (discussing use of e-mail).

84. *See* David J. Goldstone, *A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech*, 69 U. COLO. L. REV. 1, 10 (1998) (suggesting that cyberspace is analogous to city that has numerous fora rather than single unitary forum and analogizing e-mail and Web to neighborhoods).

85. *See* ACLU v. Reno, 31 F. Supp. 2d 473, 498 (E.D. Pa. 1999) (granting plaintiff's motion for preliminary injunction against enforcement of Child Online Protection Act (COPA) on grounds that COPA violates First Amendment); Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists, 23 F. Supp. 2d 1182, 1195 (D. Or. 1998) (denying defendant's motion for summary judgment because issue of material fact existed as to whether Web page constituted "true threat" against abortion services providers). The *Planned Parenthood* case recently went to trial and ended with a $107 million jury verdict for the plaintiffs. *See* Adam Cohen, *Cyberspeech on Trial*, TIME, Feb. 15, 1998, at 52, 52 (discussing verdict).

86. *See* Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521, 531 (1998) (observing that Internet "law" did not truly develop until after 1996, despite Internet's rapid growth). The Internet's growth began with the introduction of Mosaic browser software in 1993. *Id.* Early Internet users seemed to prefer self-regulation. *Id.* at 532. Thus, the lack of case law is not surprising. For a brief discussion of the self-regulating nature of the early Internet, see Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 BERKELEY TECH. L.J. 233, 254 (1996); Richard C. Lee, Cyber Promotions, Inc. v. America Online, Inc., 13 BERKELEY TECH. L.J. 417, 424 (1998). Other commentators also have discussed how rules for regulating the Internet have arisen. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1015-25 (discussing ways in which rules for regulating Internet have

paucity of case law led the first courts addressing issues arising from Internet activity simply to analogize Internet issues to issues in existing law as a basis for decision making,[87] but the courts often failed to examine and to fully understand the underlying activity actually occurring on the Internet.[88] In failing to distinguish among various Internet activities, the courts did not adequately address factual differences among the cases that might have led to different and more consistent results.[89]

Some of the first Internet-related cases addressed the threshold question of whether courts could exercise personal jurisdiction over nonresident defendants.[90] Initially, some courts found that a party's mere presence on the Web by maintaining a Web site amounted to sufficient contact to allow the exercise

---

arisen); Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMMLAW CONSPECTUS 181, 183 (1997) [hereinafter Lessig, *The Constitution of Code*] (outlining ways in which norms regulate behavior in cyberspace).

87. *See* Geist, *supra* note 86, at 532 (noting that courts addressed early cases involving Internet with uncertainty). A Wisconsin court refused to extend the state's libel statute definition of "periodical" to include a computer network bulletin board. *Id.* (citing It's in the Cards, Inc. v. Fuschetto, 535 N.W.2d 11, 14-15 (Wis. Ct. App. 1995)). The Wisconsin court decided that because of the rapid changes and growth of technology, expanding the statutory definition of "periodical" would amount to judicial legislating. *It's in the Cards, Inc.*, 535 N.W.2d at 14-15; *see* Geist, *supra* note 86, at 532 (commenting upon court's decision to avoid making decision about effect of computer network on libel law).

88. *See* Geist, *supra* note 86, at 533 (stating that courts did not analyze underlying activity in Internet cases but rather attempted to analogize Internet to existing legal systems). Scholars have made various analogies to existing legal paradigms including national advertising, admiralty law, Antarctica law, outer space law, and environmental litigation. *See id.* at 546; *see also* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (discussing different types of Internet activity ranging from purely passive information posting to clearly conducting commercial transactions). The federal district court in *Zippo* also stated that there is a middle ground "occupied by interactive Web sites where a user can exchange information with the host computer." *Id.* The court further explained that "exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site." *Id.*

89. *See* Christopher W. Meyer, Note, *World Wide Web Advertising: Personal Jurisdiction Around the Whole Wide World?*, 54 WASH. & LEE L. REV. 1269, 1301-02 (1997) (suggesting that use of either "mere placement" test or "additional conduct" test for assessing personal jurisdiction is too rigid and that courts need to use more flexible test to analyze minimum contacts in Web setting). Meyer discusses the different tests that courts have applied to jurisdictional analysis using Web advertising contacts. *Id.* at 1300-23.

90. *See infra* notes 91-92 (listing early cases involving jurisdictional questions). Courts may exercise personal jurisdiction over a defendant when the defendant has sufficient minimum contacts with the forum such that the exercise of jurisdiction comports with notions of "fair play and substantial justice." International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)). The standard is flexible and thus allows courts to analyze new types of contacts and combinations in order to find personal jurisdiction. *See* Meyer, *supra* note 89, at 1271 (discussing flexibility of personal jurisdiction standard).

of personal jurisdiction over the nonresident defendant.[91] However, the courts soon began to recognize that mere Web presence without more was not enough to warrant an exercise of personal jurisdiction over nonresident defendants.[92] Courts acknowledged that the "nature and quality"[93] of the conduct over the Internet, rather than mere presence on the Internet, should affect the determination of personal jurisdiction.[94]

Beyond the question of jurisdiction, courts have addressed a variety of complaints arising from the Internet.[95] Important cases have concerned ISP

91. *See* Digital Equip. Corp. v. AltaVista Tech., Inc., 960 F. Supp. 456, 462 (D. Mass. 1997) (recognizing that minimum contacts with forum included Web site); Cody v. Ward, 954 F. Supp. 43, 47 (D. Conn. 1997) (finding personal jurisdiction based in part on e-mail sent to forum); Heroes, Inc. v. Heroes Found., 958 F. Supp. 1, 5 (D.D.C. 1996) (exercising jurisdiction based on newspaper ad but commenting upon importance of defendant's Web contacts); EDIAS Software Int'l, L.L.C. v. BASIS Int'l Ltd., 947 F. Supp. 413, 422 (D. Ariz. 1996) (finding minimum contacts from e-mail and Web use); Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 165 (D. Conn. 1996) (using Web presence as contact for finding personal jurisdiction over nonresident defendant); Humphrey v. Granite Gate Resorts, Inc., 568 N.W.2d 715, 720 (Minn. Ct. App. 1997) (finding jurisdiction based on gambling page on Web).

92. *See* Cybersell, Inc. v. Cybersell Inc., 130 F.3d 414, 419-20 (9th Cir. 1997) (holding that defendant's Web site did not amount to purposeful availment for personal jurisdiction); Weber v. Jolly Hotels, 977 F. Supp. 327, 333 (D.N.J. 1997) (declining to find personal jurisdiction based solely on Internet presence); Hearst v. Goldberger, 96-Civ. 3620, 1997 WL 97097, at *3 (S.D.N.Y. Feb. 26, 1997) (same); Bensusan Restaurant Corp. v. King, 937 F. Supp. 295, 301 (S.D.N.Y. 1996) (same). *See generally* Howard B. Stravitz, *Personal Jurisdiction in Cyberspace: Something More is Required on the Electronic Stream of Commerce*, 49 S.C. L. REV. 925 (1998) (discussing modern jurisdictional doctrine and how courts use it in connection with Internet cases); Meyer, *supra* note 89 (arguing for restraint in courts' attempts to use nonresident defendants' Web advertising activities as basis for personal jurisdiction).

93. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997). In *Zippo*, the court examined several cases discussing the relationship between Web sites and personal jurisdiction. *Id.* at 1123-25. The court stated that the likelihood that a court may exercise personal jurisdiction over a defendant is directly proportional to the nature and quality of the commercial activity that the defendant conducts via the Internet contact in question. *Id.* at 1124. In *Zippo*, the defendant actually conducted business on its Internet site by selling passwords to subscribers to its Web service. *Id.* at 1125-26. The court found that by doing business over the Web page, rather than merely advertising its business, the defendant's activities constituted purposeful availment of the benefits of doing business in the forum state. *Id.* After considering the other prongs of the test for jurisdiction, the court determined that jurisdiction was proper. *Id.* at 1126-27.

94. *See id.* at 1124 (finding that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet"); *see also* Geist, *supra* note 86, at 540 (stating that courts have changed focus in jurisdictional analysis to focus on nature and quality of commercial activity on Internet). Courts have realized that Internet activity is as varied as daily life. *Id.* at 538. Thus, courts can no longer categorize all Internet activity as one type of activity fitting into one analogy. *Id.*

95. *See infra* notes 96-100 and accompanying text (discussing various issues that have arisen from Internet cases).

liability for defamatory statements that the ISP's subscribers posted on network bulletin boards.[96] Other Internet-related cases have applied the First Amendment,[97] interpreted federal statutes,[98] applied harassment and employment laws,[99] and protected privacy rights.[100]

---

96. *See* Zeran v. America Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (finding commercial ISP to be publisher within meaning of Communications Decency Act, 47 U.S.C. § 230(c)(1) (Supp. II 1996), and thus, 47 U.S.C. § 230(c)(1) protected defendant from liability for defamatory statements that ISP subscriber posted on defendant's service); Blumenthal v. Drudge, 992 F. Supp. 44, 52-58 (D.D.C. 1998) (granting summary judgment to defendants in defamation action against ISP); Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (finding CompuServe to be distributor, not publisher, of information available on its computer network "forums," thus, applicable standard of liability was that of distributor, not publisher). According to *Zeran*, 47 U.S.C. § 230(c)(1) immunizes ISPs from liability for information posted by third parties. *Zeran*, 129 F.3d at 328. *But see* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, *7 (N.Y. Sup. Court., May 24, 1995) (holding ISP liable as publisher for defamatory statements that unidentified third party made); *see also* Meyerson, *supra* note 2, at 140-45 (discussing early cases and law about ISPs' liability for speech carried on their services); Development: III, *The Long Arm of Cyber-reach*, 112 HARV. L. REV. 1610, 1612-22 (1999) (discussing development of defamation actions arising from information posted on Internet Web pages).

97. *See* Mainstream Loudoun v. Board of Trustees, 2 F. Supp. 2d 783, 795 (E.D. Va. 1998) (using First Amendment analysis and holding that public library could not adopt and enforce content-based restrictions to block access to Internet sites featuring obscenity or child pornography absent compelling state interest and means narrowly tailored to end); Urofsky v. Allen, 995 F. Supp. 634, 643-44 (E.D. Va. 1998) (holding that statute limiting state employee access to sexually explicit materials violated First Amendment), *rev'd sub nom.* Urofsky v. Gilmore, 167 F.3d 191, 196 (4th Cir. 1999).

98. *See* United States v. Baker, 890 F. Supp. 1375, 1388 (E.D. Mich. 1995) (examining e-mail for content that is necessary to constitute "true threat" in interstate commerce under 18 U.S.C. § 875(c) (1994)); *see also* Sally Greenberg, *Threats, Harassment, and Hate On-Line: Recent Developments*, 6 B.U. PUB. INT. L.J. 673, 680 (1997) (discussing development of law regarding threats of physical violence and usefulness in applying such law to threats transmitted on-line). Consider also the threat that a Florida youth recently sent via the Internet to a current student at Columbine High School in Littleton, Colorado. *Internet Threat Closes Columbine High School*, N.Y. TIMES, Dec. 17, 1999, at A27. This threat has resulted in a federal indictment. *2 Indicted, 1 Probed in Columbine Threats*, DENV. POST, Jan. 11, 2000, at A09.

99. *See* Owens v. Morgan Stanley & Co., 1997 WL 793004, at *1-*4 (S.D.N.Y. Dec. 24, 1997) (explaining background of suit against employer after employee received racist e-mail at work); Bohach v. Reno, 932 F. Supp. 1232, 1236-37 (D. Nev. 1996) (finding that employer's reading of employees' electronic messages did not violate privacy laws). For a discussion of employer's potential liability for employee e-mail, see Henry H. Perritt, Jr., LAW AND THE INFORMATION SUPERHIGHWAY § 4.30A (Supp. 1999). Discussing the effect of the Internet on labor law, one commentator explains that the Internet has not changed the application of existing law. *See* Geist, *supra*, note 86, at 557-58. Rather, the Internet has added a medium of communication and facilitated the potentially offensive activity. *Id.* Thus, the application of the law in a workplace harassment case will be the same whether the harassment was through an e-mail or a paper memo. *Id.*

100. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 459 (5th Cir. 1994) (stating that federal district court had determined that Secret Service violated Privacy

### 2. The Supreme Court and the Internet

Because of the potentially intrusive nature of computers, akin to "Orwellian mischief,"[101] several United States Supreme Court Justices have expressed concern over the potential effects of computers on civil liberties and criminal law.[102] In spite of the reservations of some of its members, the Court has increasingly accepted the importance of new technology.[103] However, the

---

Protection Act when it read e-mail stored on properly seized computer system); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding that company's interception of employee e-mail received over employer's computer system did not constitute violation of employees' privacy); *see also* Pritchard, *supra* note 73, at 240-43 (discussing case law on e-mail and privacy); Sundstrom, *supra* note 77, at 2064-67 (commenting upon frequency of e-mail monitoring in workplace).

101. Arizona v. Evans, 514 U.S. 1, 25 (1995) (Ginsburg, J., dissenting) (quoting Arizona v. Evans, 866 P.2d 869, 872 (Az. 1994)).

102. *See* Sampson v. Murray, 415 U.S. 61, 96 n.2 (1974) (Douglas, J., dissenting) (commenting about effects of computers and suggesting that "we live in an Orwellian age" in which computers are turning society into transparent world); *see also* United States v. Jacobsen, 466 U.S. 109, 138 (1984) (Brennan, J., dissenting) (warning that Court's holding in Fourth Amendment case would permit "technology to override the limits of law in the area of criminal investigation"); Jeff Bleich & Kelly Klaus, *Hurtling into Cyberspace: As the Court Guides New Technology Through Old Law – Expect a Few Bumps*, 45 FED. LAW. 38, 40 (1998) (commenting on Supreme Court's attitude toward computer technology and how Court's attitude has been changing).

103. *See* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 742 (1996) (acknowledging role of technology in determining what standard of review to apply). In his plurality opinion, Justice Breyer refused to choose a specific level of First Amendment review for government regulation on cable television. *Id.* "[A]ware as we are of the changes taking place in the law, the technology, and the industrial structure, related to telecommunications, we believe it unwise and unnecessary definitively to pick one analogy or one specific set of words now." *Id.* at 742 (citations omitted). Although the issue in *Denver Area Educational Telecommunications* was the government's attempt to regulate cable television, the opinion nonetheless demonstrates that at least some members of the Court recognize the importance of carefully selecting standards of review in the area of new technology. *Id.*; *see also* Mark S. Kende, *The Supreme Court's Approach to the First Amendment in Cyberspace: Free Speech as Technology's Hand-Maiden*, 14 CONST. COMMENTARY 465, 466-72 (1997) (discussing *Denver Area Educational Telecommunications* and analyzing legal reasoning behind it). For some interesting examples of cases in which courts have not recognized the importance of a new and emerging technology, see *Mutual Films Corp. v. Industrial Comm'n of Ohio*, 236 U.S. 230, 244 (1915), *overruled by Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495 (1952), which ruled that the Ohio Constitution does not protect motion pictures because they are merely "spectacles" and are not part of the press or of public expression; see also *Greater Fremont, Inc. v. City of Fremont*, 302 F. Supp. 652, 665 (N.D. Ohio 1968), *aff'd sub nom. Wonderland Ventures, Inc. v. City of Sandusky*, 423 F.2d 548, 549 (6th Cir. 1970), which rejected the classification of cable television as a public utility because the public's need for it is akin to the public's need for "hand carved ivory backscratchers." *See generally* The Telephone Cases, 126 U.S. 1 (1888) (marveling at telephone's ability to transmit full piano chords, sounds of other musical instruments, and even human voice).

Court has had only one opportunity directly to address Internet issues.[104]

In *Reno v. ACLU*,[105] the Court held that the provisions of the Communications Decency Act (CDA) prohibiting transmissions of "indecent" or "patently offensive" material to minors violated the First Amendment to the Constitution.[106] The Court announced that it would scrutinize the statute under the most rigid First Amendment standards.[107] The Court distinguished the Internet from traditional broadcast media,[108] which is entitled to less protection

104. *See* ACLU II, 521 U.S. 844, 849 (1997) (agreeing with lower court determination that portions of Communications Decency Act violated First Amendment). In fact, a search on Westlaw in the Supreme Court database with the term "Internet" retrieves only two cases other than *ACLU II* that mention the Internet: *National Endowment for the Arts v. Finley*, 524 U.S. 569, 605-06 (1998) (Souter, J., dissenting), which cites to *ACLU II*, and *Denver Area Education Telecommunications Consortium v. FCC*, 518 U.S. 727, 776-77 (1996), in which Justice Souter argues, in a concurring opinion, that applying the same First Amendment standards to all communication media will have immense and unknowable effects.

105. 521 U.S. 844 (1997).

106. *See* ACLU II, 521 U.S. 844, 885 (1997) (affirming district court's determination that portions of Communications Decency Act violated First Amendment). Congress enacted the Communications Decency Act (CDA) as part of the Telecommunications Act of 1996 (TCA). *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.). Congress enacted the Telecommunications Act to encourage "the rapid deployment of new telecommunications technologies." *ACLU II*, 521 U.S. at 857 (quoting language of TCA). The plaintiffs, including the American Civil Liberties Union, challenged the CDA's provisions that prohibited the transmission or display of indecent or patently offensive materials over the Internet in any manner that would permit minors to access such transmissions or displays. *Id.* at 857-61. First, the Court rejected the government's argument that the restrictions were merely time, place, and manner restrictions, because the restrictions at issue directly applied to content. *Id.* at 864-68. The Court then acknowledged that every medium of speech, including the Internet, has its own special issues. *Id.* at 868-70. Cyberspace never has been subject to the type of government regulation that has attended the broadcast media. *Id.* The Court agreed with the district court's finding that the Internet is not invasive in the same way as is television or radio. *Id.* Additionally, warnings alerting the user to sexual content appear on Web sites. *Id.* at 854. Therefore, a user is less likely to happen upon sexual content accidentally. *Id.* Furthermore, the Court observed that the Internet is not a scarce commodity and has virtually unlimited, low-cost capacity for all types of information. *Id.* at 870. Thus, the governmental regulation of the Internet will not receive the qualified First Amendment scrutiny applied to the broadcast media. *Id.* The Court then noted that the CDA's provisions diminished the free speech rights of adults. *Id.* at 874. The Court stated that the breadth of the CDA's coverage was unprecedented. *Id.* at 877. Furthermore, the provisions were not sufficiently narrowly tailored to meet the purported goal of protecting juveniles. *Id.* at 879. Consequently, the Court upheld the district court's determination that the provisions in question violated the First Amendment. *Id.* at 885.

107. *See id.* at 868 (announcing that Court would review CDA under most rigid First Amendment scrutiny).

108. *See id.* at 868-69 (distinguishing broadcast media from Internet because federal government has history of strong regulation of broadcast media but no history of regulating Internet).

from government regulation under the First Amendment because of a "bandwidth scarcity" rationale.[109] The Court stated that it intends to approach the Internet as a distinct medium of communication with its own "set of rules."[110] Its dynamic aspects, its versatility, and its democratizing value had impressed the Court.[111]

In rejecting the breadth of the CDA's content-based prohibitions,[112] the Court expressed concern that parents would not be able to allow their children to access information of which the parents approved.[113] The Court also denounced the CDA's constraints on adult speech, stating that "[t]he CDA . . . threatens to torch a large segment of the Internet community."[114] The Court

---

109. *See* Red Lion Broad. Inc. v. FCC, 395 U.S. 367, 375-77 (1969) (using rationale that scarcity of broadcast frequencies and large number of competing voices permits greater regulation of broadcast media and is consistent with First Amendment).

110. *See ACLU II*, 521 U.S. at 868-70 (stating that each medium of expression will present problems unique to that medium). The Court observed that there are "special justifications for regulation of the broadcast media that are not applicable to other speakers." *Id.* at 868. The Court stated that the rationale for regulation of broadcast media, as distinct from other media, arises from a history of extensive government regulation of broadcast medium, a scarcity of available broadcast frequencies, and the invasive nature of broadcast media. *Id.* According to the Court, those factors do not arise in the Internet context. *Id.* For the Supreme Court cases that have developed these factors, see *Turner Broadcasting System v. FCC*, 512 U.S. 622, 637-38 (1994); *Sable Communications, Inc. v. FCC*, 492 U.S. 115, 128 (1989); and *Red Lion Broadcasting Inc. v. FCC*, 395 U.S. 367, 375-77 (1969).

111. *See ACLU II*, 521 U.S. at 870 (articulating broad accessibility and unlimited capacity of Internet as conditions that distinguish Internet from traditional broadcast media). The Court said, "[t]hrough the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and news-groups, the same individual can become a pamphleteer." *Id.*; *see also* Kende, *supra* note 103, at 475 (commenting that Supreme Court seemingly has embraced Internet as positive social force).

112. *See* Communications Decency Act, 47 U.S.C. § 223(a), (d) (Supp. 1997) (prohibiting transmission of indecent material to recipient known to be under 18 years old). Congress stated that the purpose of the Telecommunications Act was to "encourage the rapid deployment of new telecommunications technologies." *ACLU II*, 521 U.S. at 857 (quoting Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996)). The Act primarily deals with competition in local telephone, multichannel video, and over-the-air broadcasting markets, however, and not the Internet. *Id.* at 857-58. In fact, the CDA was only one of seven titles in the Telecommunications Act. *Id.* at 858. The CDA prohibited transmissions of "indecent" or "patently offensive" material that would be accessible to minors. *Id.* at 859.

113. *See ACLU II*, 521 U.S. at 878 (stating that overbreadth of CDA's prohibitions would inhibit even parental controls of their children's Internet access). The Court expressed concern that a speaker could not "confidently assume that a serious discussion about birth control practices, homosexuality . . . or the consequences of prison rape would not violate the CDA." *Id.* at 871.

114. *Id.* at 882. The Court agreed with the district court's conclusion that the CDA's restrictions unduly burdened protected free speech. *Id.*

asserted that it would consider it inappropriate to constrain unnecessarily adult communication over the Internet.[115] Last, the Court rejected the Government's argument that the CDA would foster the unfettered growth of the Internet, concluding instead that given the already exponential growth of the Internet, the presence of pornography or adult content likely would not hinder the growth of the medium.[116]

Given the Court's approach to the Internet as a medium distinct from other communications media,[117] lower courts might follow the Court's lead and approach Internet issues as not necessarily identical to, although related to, other areas of the law. Perhaps the Court's lead will result in lower courts' approaching different Internet-related issues as discrete. The Court's approach might allow lower courts to apply varying theories to issues arising within the same method of Internet communication. For example, a court might apply a contract theory to one type of e-mail contact,[118] while applying a tort theory to another type of e-mail contact.[119] In sum, the newness of the Internet demonstrates that courts have ample opportunity for creative application of the common law.[120] Scholarly reaction has been no less diverse than the courts' reactions.[121]

---

115. *See id.* at 874-79 (discussing unacceptability of restrictions on adult speech when less restrictive alternatives could achieve purported purpose of statute).

116. *See id.* at 885 (rejecting Government's assumption that content regulation is necessary to promote Internet expansion). The Government argued that people would eventually stop using the Internet because of the presence of pornography. *Id.* The Court found the Government's argument "singularly unpersuasive" given that the record had demonstrated phenomenal growth, not contraction. *Id.*

117. *See id.* at 851 (recognizing Internet as communication medium comprised of many methods of communication and information retrieval). The Court commented that cyberspace is not located in any particular geographic space, but users anywhere in the world can access its resources through the Internet. *Id.*

118. *See* CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1260-61 (6th Cir. 1996) (explaining contract action based on electronic transmissions).

119. *See* America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (finding liability for common-law tort of trespass to chattels when advertiser spammed ISP's customers); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020 (S.D. Ohio 1997) (granting preliminary injunction to ISP based in part on common law theory of trespass to chattels).

120. *See* Doug Rendleman, *Common Law Restitution in the Mississippi Tobacco Settlement: Did the Smoke Get in Their Eyes?*, 33 GA. L. REV. 847, 859 (1999) (stating that adapting "to economic and cultural change is also one of the common law's features"). Rendleman also makes the point that being flexible and tailoring solutions to particular disputes are features of the common law. *Id.* However, when society changes rapidly, earlier precedential decisions may hold little sway or may be wrong. *Id.* As applied in the context of the Internet, applying the common law will allow the courts to be flexible to issues arising from the rapidly changing technology.

121. *See infra* Part III.B (discussing various commentators' views on approaches to development of Internet law).

### *B. Commentators' Views*

Scholars and commentators have taken a variety of approaches to the issue of Internet regulation.[122] Some scholars have argued that traditional legal notions regarding physical space will not properly apply to regulating the Internet.[123] These scholars argue that Internet interactions crossing territorial boundaries have created a new and discernable space.[124] Because this new medium does not confine itself to geographical boundaries, territorially based sovereigns cannot adequately regulate cyberspace activities.[125] Thus, according to these scholars, this new "territory" of cyberspace demands its own law.[126]

---

122. *See infra* notes 123-32 and accompanying text (discussing various approaches to Internet regulation).

123. *See* David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378-81 (1996) (arguing that traditional notions of legal regulation will not work in cyberspace context); Katsh, *supra* note 66, at 1685-92 (suggesting that differentiations between electronic space and print space should result in orientation of First Amendment in cyberspace around "electronic" space rather than print space). The crux of Post's and Johnson's argument is that traditional legal notions are grounded in physical borders and that without those borders it will be impossible to govern cyberspace in the same manner as the physical world. *Id.* at 1378-80; *see also* John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L. J. 207, 234 (1997) (criticizing attempts at regulating Internet and characterizing them as being parochial and overly limiting); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, *in* BORDERS IN CYBERSPACE 84, 96-100 (Brian Kahin & Charles Nesson eds., 1997) (arguing that borders marking national sovereignty will not suffice for determining which government should govern network issues, and that new network governance paradigm must emerge to establish norms of conduct for computer networks). *But see* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200-1201 (1998) (arguing against Post's and Johnson's conclusion that "real space" law cannot properly apply to cyberspace).

124. *See* Johnson & Post, *supra* note 123, at 1367, 1378-81 (stating that cyberspace is distinct place for purposes of legal analysis). Post and Johnson posit that cyberspace users know when they have entered the "other space" because of the process it takes to get there – passing through a "border" of computer screens and passwords. *Id.* at 1379.

125. *Id.* at 1375. The authors explain that because physical boundaries do not separate Internet activities, no particular jurisdiction has a compelling claim exclusively to subject Internet users to that jurisdiction's laws. *Id.* Another scholar suggests that government regulation should differ according to the particular Internet activity that the state seeks to regulate. *See* Steven R. Salbu, *Who Should Govern the Internet?: Monitoring and Supporting a New Frontier*, 11 HARV. J. L. & TECH. 429, 441-52 (1998) (positing that propriety of state government power to regulate cyberspace depends upon type of activity that state seeks to regulate). Salbu argues that some activities should not be subject to state regulation simply because there is no "local" interest in regulating the behavior. *Id.* at 441-42. At the other end of the spectrum, Salbu observes that some Internet activities are "so novel that they create unique regulatory challenges. Other facets of the Internet may create a new spin on an old theme." *Id.* at 441.

126. *See* Johnson & Post, *supra* note 123, at 1387 (explaining that because authors call for legal authority not based in geographic territory, it will be necessary to create new legal institutions to govern cyberspace).

Another scholar has urged courts and legislatures to take a restrained approach to regulating the Internet,[127] suggesting that cyberlaw, law specific to the Internet, should develop as has all common law, with incremental changes that lead slowly to more fundamental changes.[128] In addition, some scholars have suggested that change to existing law is not necessary and that Internet regulation issues are analogous to issues arising in other legal contexts.[129] These scholars have concluded that existing legal schemes will provide the answers to the dilemmas of Internet regulation.[130] Finally, some scholars have suggested that the limitations of the technology itself can be the source of the regulatory framework.[131] Thus, they have argued that new regulations will not be the only or the best source of regulation because the natural constraints of the technology will better regulate the activity.[132]

The scholarship has encouraged the courts to consider more creative applications of the law. In discussing how to regulate the Internet, if at all, commentators are suggesting that the courts emphasize the nature and quality of the Internet contacts.[133] Thus, the courts should not approach all Internet-related cases as identical to each other, and courts should refrain from ap-

127. *See* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1744 (1995) (urging approach to cyberspace regulation that will let "experience catch up with the technology").

128. *See id.* at 1745 (suggesting that common law's "constructive function" will allow law to develop as understanding of medium develops). Lessig argues that First Amendment jurisprudence particularly should respond slowly. *Id.* at 1752-53. He predominantly is interested in the Court's allowing the salient issues to develop fully before trying to "ventur[e] too boldly into [the Internet's] regulation." *Id.* at 1752; *cf.* Keller, *supra* note 70, at 427 (observing that it is unrealistic to expect statutory law to be able to keep up with changes in computer technology and that common law will be more responsive to changes).

129. *See* Geist, *supra* note 86, at 546 (stating that scholars have made various analogies to existing legal paradigms including national advertising, admiralty law, Antarctica law, outer space law, and environmental litigation).

130. *See id.* at 546-47 (listing variety of situations and paradigms to which scholars have compared Internet).

131. *See id.* at 549 (observing that commentators are recognizing limits of technology itself as way to determine what and how to regulate Internet); Lessig, *The Constitution of Code*, *supra* note 86, at 183-84 (suggesting that nature of technology will permit technology to be indirect regulatory framework for Internet); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554-55 (1998) (positing that "[t]echnological capabilities and system design choices impose rules on participants" over and above those that law and government regulation impose).

132. *See* Lessig, *The Constitution of Code*, *supra* note 86, at 185-86 (suggesting that computer technology limitations will assist regulation because it provides additional indirect regulation); Reidenberg, *supra* note 131, at 577-86 (suggesting ways in which information technology will provide rules for regulating cyberspace).

133. *See* Geist, *supra* note 86, at 548-49 (commenting on trend in legal scholarship toward analysis of nature and quality of activity on Internet before categorically reaching given result).

proaching Internet-related cases as cases that are wholly distinct from other areas of law. Furthermore, within the context of the Internet, the nature and quality of the contacts differ from e-mail to e-mail and from e-mail to the Web. By considering the nature and quality of Internet activity, courts can develop law that is responsive to specific e-mail issues, for example, rather than reflective of a blanket application of a single paradigm to all Internet-related issues.

### *IV. Commercial ISPs, E-Mail, and Spam*

Various causes of action arising from Internet activities have presented interesting issues for the Supreme Court, lower courts, and commentators to consider.[134] However, even more interesting than the issues themselves are the particular contexts in which the Internet issues arise.[135] For example, the *Intel* case provides an opportunity to examine how private network providers can protect their interests in their networks.[136] To help the reader understand how the court approached Intel's problem with the unwanted e-mail from Hamidi and FACE Intel, this Part examines the ways in which commercial network owners, ISPs, have protected their interests.

### *A. The Problem of Spam*

The Internet is becoming increasingly commercial as businesses are advertising their wares on their own Web pages, on others' Web pages, and by e-mail sent directly to consumers.[137] When advertisers pay for access to

---

134. *See supra* Part III (discussing courts' and scholars' approaches to Internet).

135. *See supra* notes 95-100 and accompanying text (discussing examples of different Internet-related litigation).

136. *See infra* Part V.C (proposing limited application of trespass to land to protect private network provider's interest); *infra* notes 154-59, 194-96 and accompanying text (explaining inadequacy of trespass to chattels for protecting interest and placing explanation in context of *Intel*); *infra* notes 248-55 and accompanying text (discussing importance of private network provider's interest in network).

137. *See* William J. Holstein, et al., *Click 'Til You Drop*, U.S. NEWS & WORLD REPORT, Dec. 7, 1998, at 42 (discussing increasing use of Internet to buy goods). The article observes that because of the federal government's current "wait and see" policy with respect to taxing online purchases, the numbers are likely to continue to grow. *See id.* at 44; *see also* Meyer, *supra* note 89, at 1281-85 (providing in-depth discussion of different Web advertising methods and practices); Kavita Kaur, *The Net: It's Clicked, But Will It Hit?*, COMPUTERS TODAY, Nov. 30, 1998, at 74 (stating that market researchers have estimated that Internet advertisements will account for approximately 11% of global revenues). In two cases, the ISP estimated that it had received up to 60 million e-mail advertisements. *See* America Online, Inc. v. IMS, Inc., 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (stating that ISP had received 60 million pieces of e-mail advertising over ten-month period); Cyber Promotions, Inc. v. American Online, Inc., 948 F. Supp. 436, 438 (E.D. Pa. 1996) (discussing ISP's contention that its customers had received

consumers by paying an ISP for Internet access or by paying a Web page creator for space on its page, few problems arise.[138] Problems do arise, however, when advertisers access potential consumers by e-mail without paying for access to those consumers.[139]

Recently, the courts have addressed disputes between commercial ISPs and advertisers who have "spammed" the ISPs' customers.[140] "Spam" is the term for unsolicited, bulk e-mail messages.[141] Spam has created problems because some ISPs do not want to fund third-party advertisements to their

---

literally millions of unsolicited bulk advertising e-mail messages from advertiser). Note that the Federal Supplement incorrectly lists America Online as American Online. *Id.*

138. *See* Carroll, *supra* note 86, at 265-68 (explaining that problems arise because ISPs must bear costs of advertising another's product); David E. Sorkin, *Unsolicited Commercial E-mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1006-1012 (1997) (addressing costs to unsolicited bulk e-mail in dollars, time, and resources).

139. *See* Carroll, *supra* note 86, at 234 (commenting upon relatively low costs of e-mail). Carroll seems particularly concerned that "junk e-mail" threatens the viability of an entire mode of communications. *Id.* "Because the marginal costs of producing and distributing electronic junk mail are very low, the incentives for advertisers to flood the network with unsolicited commercial solicitations are substantial. Left unchecked, this flood of advertisements could produce a tragedy of the commons." *Id.*; *see* Leibowitz, *supra* note 4, at 10 (stating that America Online has filed nine lawsuits in five states to stop unsolicited bulk e-mail from coming onto its system).

140. *See* America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998) (discussing ISP's allegation that unauthorized e-mail messages violated Lanham Act and Virginia common law of trespass to chattels and nuisance); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020 (S.D. Ohio 1997) (explaining plaintiff's claim of trespass to personal property or chattels when advertiser sent mass amount of unsolicited e-mail to ISP's customers); Cyber Promotions, Inc. v. American Online, Inc., 948 F. Supp. 436, 437-38 (E.D. Pa. 1996) (noting defendant's argument for right to send unsolicited commercial e-mail to ISP's customers).

141. *See CompuServe*, 962 F. Supp. at 1018 (acknowledging that different parties refer to mass commercial e-mail as either "bulk e-mail" or "junk e-mail" and that Internet vernacular calls such e-mail "spam"); Goldstone, *supra* note 84, at 11 (defining spam as mass advertising e-mail); Anne. E. Hawley, Comment, *Taking Spam out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, 66 U. MO.-K.C. L. REV. 381, 381 & n.3 (1997) (explaining that spamming is sending bulk unsolicited commercial e-mail). *See generally* Sorkin, *supra* note 138 (discussing possible methods of regulating unsolicited commercial e-mail, or junk e-mail, under existing statutory regimes and alternatives); Steven E. Bennett, Note, *Canning Spam:* CompuServe, Inc. v. Cyber Promotions, Inc., 32 U. RICH. L. REV. 545 (1998) (discussing efforts by courts and legislatures to eliminate or regulate junk e-mail). According to the court in *CompuServe*, the term spam "derive[s] from a skit performed on the British television show Monty Python's Flying Circus, in which the word 'spam' is repeated to the point of absurdity in a restaurant menu." *CompuServe*, 962 F. Supp. at 1018 n.1. Most references to spam refer to spam as unsolicited, bulk, *commercial* e-mail; however, there is little reason that the term cannot apply equally to any unsolicited bulk e-mail. *See* Sorkin, *supra* note 138, at 1003 n.16 (discussing both commercial and noncommercial unsolicited bulk e-mail, or "spam").

customers.[142] In order to reduce their own costs and to keep their customers happy, ISPs need to be able to stop advertisers from sending unsolicited bulk e-mail over the ISPs' systems to the ISPs' customers.[143] To stop the advertisers, some ISPs have sued the senders of the unsolicited e-mail on the basis of a trespass to chattels theory.[144]

### *B. Trespass to Chattels May Provide a Theory to Combat Spam*

In winning cases against spammers, some ISPs have argued that spam constitutes a trespass to chattels because it is an intermeddling with a chattel in another's possession.[145] Under traditional doctrine, an actor can commit a

---

142. *See* Goldstone, *supra* note 84, at 48-52 (addressing costs of unsolicited, commercial e-mail as being economic externality by imposing costs on recipients); Sorkin, *supra* note 138, at 1019 (commenting on sender's shifting advertising costs to recipient of junk e-mail or recipient's ISP); Hawley, *supra* note 141, at 382 (discussing increasing costs of spam, including consumption of computer resources); *see also* Lee, *supra* note 86, at 427 & n.67 (observing that costs of storage of mass numbers of e-mail messages fall on recipient ISP and are most expensive aspect of e-mail transmissions); *cf.* Carroll, *supra* note 86, at 272-74 (arguing against use of government regulation to shift costs of unsolicited commercial e-mail back to senders on ground that there is no clear government interest in preventing cost-shifting).

143. *See* Lee, *supra* note 86, at 427 n.66 (listing costs to receiving ISP for e-mail message storage before recipient's retrieval, recipient's retrieval of messages, and recipient's deletion or storage of messages). Although ISP subscribers also bear some costs, such as having to pay for the time it takes to delete unwanted mail, these costs are minimal. *Id.* at 426; *see* Goldstone, *supra* note 84, at 48-50 (discussing various costs that sorting and storing e-mail impose upon ISPs and receiving networks); Sorkin, *supra* note 138, at 1010 (stating that costs of receiving e-mail generally are borne more by ISPs than by individual users). Sorkin notes that some of the antipathy to commercial e-mail results from the non-commercial origins of the Internet. *Id.* at 1007. He states that the "economics of the Internet are also of little help: it can be cheaper to send an advertising message everywhere than to target it to a narrow group of prospects, and it may be more effective [than hoping recipients] . . . will search out the advertiser's home page on the Web." *Id.* at 1007-08. For a list of over fifteen cases that ISPs have filed against spammers, see The John Marshall Law School, Center for Information Technology & Privacy Law, *Unsolicited E-mail: Cases* (visited Jan. 14, 2000) <http://www.jmls.edu/cyber/cases/spam.html>.

144. *See America Online*, 24 F. Supp. 2d at 552 (granting plaintiff's motion for summary judgment for claim of trespass to chattels when defendant sent unauthorized bulk commercial e-mail over plaintiff's computer network); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1028 (S.D. Ohio 1997) (finding that plaintiff could maintain action for trespass to chattels).

145. *See America Online*, 24 F. Supp. 2d at 552 (granting plaintiff's motion for summary judgment for claim of trespass to chattels when defendant sent unauthorized bulk commercial e-mail over plaintiff's computer network); *CompuServe*, 962 F. Supp. at 1028 (finding that plaintiff could maintain action for trespass to chattels). For additional cases applying trespass to chattels and conversion to "modern" facts, see *United States v. Arora*, 860 F. Supp. 1091, 1098-99 (D. Md. 1994), which applies conversion and trespass to chattels theories to a case in which a doctor interfered with the creation of "human cell lines" in a research project, and

trespass to chattels by using or intermeddling with a chattel that is in the possession of another.[146] An actor intermeddles by intentionally bringing about physical contact with the chattel.[147] The requisite intent exists if the actor commits the act with the purpose of intermeddling or with the knowledge that intermeddling may result from the act.[148] However, if an actor has consent from the possessor to intermeddle with the chattel, then no cause of action will arise.[149] The possessor of the chattel can limit or revoke the consent,[150] and if the actor exceeds the scope of the consent, then a cause of action for trespass to chattels will arise.[151] Furthermore, in some instances a privilege, irrespective of consent, might insulate an actor from liability for trespass to chattels.[152] Privileges include the use of public utilities, the defense of land or chattels, self defense, and public necessity.[153]

A plaintiff also must prove that the actor's interference caused harm.[154] When the actor has impaired the condition, quality, or value of the chattel, the actor will be liable only for the harm to a materially valuable interest in the physical condition, the quality, or the value of the chattel.[155] Unlike a trespass to real property, the law does not provide recovery for nominal damages when

---

*Moore v. Regents of University of California*, 793 P.2d 479, 493-97 (Cal. 1990), which found that a doctor was not liable for conversion when the doctor had harvested cells from patient's body without informing the patient.

146. RESTATEMENT (SECOND) OF TORTS § 217(b) (1965).

147. *See id.* § 217 cmt. e (explaining trespass as either act that brings actor into physical contact with chattel in possession of another or act that results in directing object at chattel in possession of another).

148. *See id.* § 217 cmt. c (explaining character of intent necessary to maintain action for trespass to chattels). Knowledge as to any interference with the possessory right of another is not necessary. *Id.*

149. *See id.* §§ 218 cmt. b, 252 & cmt. b (explaining that if actor has consent from owner then actor will not be liable for trespass to chattels).

150. *See id.* § 252 cmt. c (observing that possessors of chattel may limit consent to specific time, place or other condition of use); *id.* § 254 & cmt. a (stating that possessor may terminate actor's privilege to intermeddle with chattel in question).

151. *See id.* § 252 cmt. c (stating that acting outside scope of limited privilege that possessor has granted may result in liability for harm to chattel).

152. *See id.* §§ 259-278 (discussing privileges that might protect actor from liability for use of chattel of another).

153. *See id.* § 259 (providing for privilege of use of public utility); *id.* § 260 (providing for privilege of defense of land or chattels); *id.* § 261 (providing privilege for defending self or third person); *id.* § 262 (providing privilege for acts done because of public necessity).

154. *See id.* § 218 cmt. e (stating that possessor must show actor caused actual harm).

155. *Id.* An actor also can be liable for harm that arises if the actor dispossesses the possessor of the chattel, deprives the possessor of use of the chattel for a substantial time, or if bodily harm comes to the possessor or a person or thing in which that possessor has a legally protected interest. *Id.* § 218(a), (c)-(d).

the intermeddling with the chattel is harmless.[156] Furthermore, the possessor has a privilege to use reasonable force to protect a chattel from harmless interference.[157] Thus, the law reasons, the privilege to use reasonable force provides the possessor with sufficient legal protection of the interest in the personal property.[158]

Several cases have established and confirmed that electronic signals are physical contacts sufficient to give rise to a claim for trespass to chattels.[159] Thus, when an actor has sent an unwanted e-mail or other electronic signal to a network, ISPs or other computer network owners can overcome the initial requirement that an actor has intermeddled with the chattel. The more difficult hurdle involves proving the damages to the computer network owner's interest in the chattel.

### *C. Early Application of Trespass to Chattels to Computer Technology*

Analogizing invasions of computer systems to trespass to chattels has its origins in the 1996 California case of *Thrifty-Tel, Inc. v. Bezenek*.[160] In *Thrifty-Tel*, two minors used computer technology and stolen codes to access the plaintiff's telephone system in order to make unauthorized long-distance telephone calls.[161] The California Court of Appeal for the Fourth District determined that the minors' acts constituted a trespass to personal property, or chattels.[162] At the trial court, the plaintiff in *Thrifty-Tel* originally won on

---

156. *Id.* § 218 cmt. e. The *Restatement* gives the example of the child who pulls a dog's ears. In such a case, the child has done no harm to the dog or to a legally protected interest of the owner. *Id.* § 218 cmt. e, illus. 2. Thus, the actor is not liable to the owner of the dog. *Id.* That the law does not protect the owner's interest in the mere inviolability of a chattel is in contrast to the law's protection of a land-owner's interest in the mere inviolability of the land. *Id.* § 218 cmt. e.

157. *See id.* §§ 77, 218 cmt. e (explaining that possessor of chattel has privilege to use reasonable force to protect interest in inviolability of chattel as against another person).

158. *See id.* (stating that privilege to use reasonable force to protect chattels provides sufficient protection interest in inviolability of chattel).

159. *See* America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (stating that unauthorized sending of bulk commercial e-mail constituted trespass to chattels); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (stating that electronic signals or messages provide sufficient contact to give rise to action for trespass to chattels); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 n.6 (Ct. App. 1996) (concluding that electronic signals generated by computers that minors used to access plaintiff's telephone system were sufficiently tangible to maintain action for trespass to personal property).

160. 54 Cal. Rptr. 2d 468 (Ct. App. 1996).

161. *See* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 471 (Ct. App. 1996) (describing minors' activities).

162. *See id.* (concluding that use of computer technology to access confidential authorization codes for plaintiff's telephone system constituted trespass to personal property). The court

a claim for conversion of personal property.[163] The defendant appealed.[164] The appellate court reversed the trial court and found that the plaintiff had failed to prove conversion because the minors did not interfere with or take a tangible interest.[165] Instead of conversion, the court found that the plaintiff had successfully proved trespass to personal property, or chattels.[166] The court stated that the electronic signals that the minors' activities generated were sufficiently tangible to support the trespass to chattels cause of action.[167]

---

concluded that computer-generated electronic signals could give rise to a cause of action for and did support liability for trespass to chattels. *Id.* In *Thrifty-Tel*, the defendants challenged the trial court's ruling that the minor children of the defendants had committed conversion. *Id.* at 472. The trial court found that the children had made unauthorized use of confidential codes to gain computer access to the plaintiff's telephone system. *Id.* at 471. The children then searched the system for authorization codes to allow them to place long distance telephone calls over the plaintiff's telephone system. *Id.* On the first occasions, the minors made manual searches of the system, and on subsequent occasions they used computer programs for between six and seven hours to search the system, generating over one thousand phone calls on plaintiff's telephone system. *Id.* The automated calling overburdened the Thrifty-Tel system and disrupted access for some subscribers. *Id.* The appellate court agreed with defendants that, traditionally, courts do not recognize conversion when there has been an unauthorized taking of intangible interests that are not merged with or reflected in something tangible. *Id.* at 472. The court, however, determined that Thrifty-Tel had pleaded and proved a cause of action for trespass to personal property, or chattels. *Id.* at 473. The court said that trespass to chattels lies when "an intentional interference with personal property has proximately caused injury." *Id.* Thus, although there was no cause for conversion, the use of the computer access and authorization codes and the tie-up of Thrifty-Tel's system constituted a trespass. *Id.*

163. *See id.* at 471 (stating that plaintiff prevailed in lower court on theories of conversion and fraud). The defendant challenged the ruling in the lower court on the grounds that the underlying facts did not support these determinations. *Id.*

164. *Id.*

165. *See id.* at 472 (agreeing that conversion did not apply to plaintiff's cause of action because defendants did not interfere with tangible interest or with intangible interest that was merged with or reflected in tangible interest). The court made the point that conversion will lie even when a defendant interferes with an intangible interest as long as the interest is merged with a tangible interest. *Id.* The court gave the example of a stock certificate, the value of which is not the tangible cost of the paper, but the intangible worth of the stock. *Id.*

166. *See id.* at 472-73 (stating that although plaintiff failed to prove conversion, court could use its recognized power to modify decision below to conclude that plaintiff had pleaded and proved claim for trespass to personal property). Furthermore, at trial, the defendants virtually conceded that the minors had trespassed. *Id.* at 472.

167. *See id.* at 472 n.6 (discussing relaxation of tangibility requirement). The court explained that although the old rule required physical touching of a tangible chattel, the more modern approach allows for an "indirect touching." *Id.* For example, dust particles or even microscopic particles may give rise to a cause of action for trespass, assuming that there is some actual physical harm to the property. *Id.* (citations omitted). The *Restatement (Second) of Torts* explains that "'intermeddling' means intentionally bringing about a physical contact with the chattel." RESTATEMENT (SECOND) OF TORTS § 217 (1965). Regardless of the relaxation of the physical contact aspects of intermeddling, the *Thrifty-Tel* court decided that the electronic

In the damages portion of the opinion, the court determined that Thrifty-Tel had failed to mitigate its damages when it had the opportunity to do so and that Thrifty-Tel had failed to establish actual damages.[168] The court rejected Thrifty-Tel's production of a statistical formula for damages reasoning that the use of statistical averaging could present a windfall to the plaintiff.[169] Furthermore, statistical averaging would not reflect the fact that some computer hacking[170] activities might only result in de minimis damages.[171]

A significant result of *Thrifty-Tel* is its recognition of electronic signals as being sufficiently physical to give rise to a cause of action for trespass to chattels.[172] Equally significant was the *Thrifty-Tel* court's recognition that not all computer hacking will give rise to an action for trespass to chattels; the court reaffirmed the notion that a claim for trespass to chattels will not be successful when the alleged damage is de minimis.[173] Thus, to recover for harm arising from an intrusion into a proprietary computer network, a plaintiff must show that the electronic intrusion actually caused some measurable harm.[174] *Thrifty-Tel* is significant because in using the common law to respond to changing technology, *Thrifty-Tel* affirmed the notion that the common law can be responsive and flexible in the face of changing technology.[175]

---

signals that the minors' activities generated were sufficient to constitute a trespass. *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 n.6.

168. *See Thrifty-Tel*, 54 Cal. Rptr. 2d at 474-75 (explaining that plaintiff failed to mitigate damages and failed to establish any actual harm). As a result of the failure to mitigate, the court determined that the plaintiffs could not recover for damages arising from any of the hacking after the first incident. *Id.* at 474.

169. *See id.* at 475 (determining that statistical formula for average damages suffered by plaintiff was not appropriate measure of damages because formula might give plaintiff windfall).

170. *See* THE AMERICAN HERITAGE DICTIONARY (3d ed. 1996) (defining "hacker" as "one who illegally gains access to or enters another's electronic system to obtain secret information or steal money").

171. *See Thrifty-Tel*, 54 Cal. Rptr. 2d at 475 (commenting that computer hacker activities vary as to amount of damages they might cause).

172. *See id.* at 473 n.6 (stating that electronic signals were sufficiently tangible to permit cause of action for trespass to chattels).

173. *See id.* at 475 (commenting that computer hacker activities vary as to amount of damages they might cause).

174. *See id.* at 474-75 (establishing that failure to prove actual harm would preclude recovery under trespass to chattels theory).

175. *See id.* at 473-74 (commenting on applying common law to modern facts); *see also* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (relying on *Thrifty-Tel* for support in finding electronic signals sufficient for trespass to chattels action). *See generally* Keller, *supra* note 70 (commenting on inadequacy of statutory regimes for regulating Internet and suggesting that common law provides best option for protecting interests as new technology develops).

### D. *Application of Trespass to Chattels to E-Mail and ISPs:* CompuServe, Inc. v. Cyber Promotions, Inc.

Using *Thrifty-Tel*'s determination that electronic signals can give rise to a cause of action for trespass to chattels,[176] an ISP brought a trespass to chattels theory claim against a spammer.[177] In *CompuServe, Inc. v. Cyber Promotions, Inc.*,[178] the United States District Court for the Southern District of Ohio granted a preliminary injunction to stop an Internet advertiser from sending bulk unsolicited commercial e-mail to the ISP's customers.[179] The case began when Cyber Promotions sent numerous unsolicited commercial e-mail messages to CompuServe's customers.[180] CompuServe's customers complained to the ISP, with some even threatening to leave CompuServe for another ISP.[181] CompuServe notified Cyber Promotions to stop sending e-mail over CompuServe's proprietary computer system.[182] Cyber Promotions responded by sending increasing volumes of the unsolicited advertisements.[183] CompuServe then attempted to block the incoming e-mail with software programs designed to filter out unwanted e-mail.[184] In turn, Cyber Promotions modified

---

176. *See* America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (stating that unauthorized sending of bulk commercial e-mail constituted trespass to chattels); *CompuServe*, 962 F. Supp. at 1021 (stating that electronic signals or messages provide sufficient contact to give rise to action for trespass to chattels); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 n.6 (Ct. App. 1996) (concluding that computer-generated electronic signals used to access plaintiff's telephone system were sufficiently tangible to maintain action for trespass to personal property).

177. *See CompuServe*, 962 F. Supp. at 1017 (agreeing that CompuServe could maintain action for trespass to chattels against online advertiser); *see also supra* Part IV.A (describing problem of spam).

178. 962 F. Supp. 1015 (S.D. Ohio 1997).

179. *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1028 (S.D. Ohio 1997) (granting plaintiff's motion for preliminary injunction).

180. *See id.* at 1017 (stating that defendant Cyber Promotions's business is to send hundreds of thousands of advertisements to Internet users by e-mail and that many Internet users are clients of CompuServe's). CompuServe is a commercial ISP that offers its service through its own proprietary computer network. *Id.* After connecting to CompuServe's network, a customer can connect to the wider resources of the Internet. *Id.*; *see supra* Part II.B (explaining how ISPs provide connections to Internet).

181. *See CompuServe*, 962 F. Supp. at 1019 (stating that CompuServe had received many complaints from its customers about e-mail advertisements that defendant sent out and stating that some customers had threatened to discontinue service with CompuServe because of large amount of bulk commercial e-mail).

182. *See id.* (explaining that CompuServe had demanded that Cyber Promotions cease and desist from sending further e-mail to CompuServe's customers).

183. *See id.* (stating that Cyber Promotions responded to demands to cease and desist from sending bulk commercial e-mail by sending large volume of additional e-mail).

184. *See id.* (explaining that CompuServe attempted to block bulk e-mail from Cyber Pro-

its own software and equipment to circumvent CompuServe's efforts to block the e-mail.[185]

Failing in its self-help efforts, CompuServe obtained a temporary restraining order.[186] CompuServe then pursued a preliminary injunction based on the common-law theory of trespass to chattels.[187] In granting CompuServe's motion for a preliminary injunction, the district court first observed that trespass to chattels was in fact an actionable tort.[188] The court found that electronic signals are "sufficiently physically tangible" to support a trespass action.[189] Furthermore, the court stated that either harm to the personal property or diminution of its value, quality, or condition would be an adequate predicate to liability.[190] The court then observed that a plaintiff who pursues

---

motions); *see also* Pritchard, *supra* note 73, at 243 (stating that one response to unwanted e-mail is to block or "kill" incoming, unwanted files).

185. *See CompuServe*, 962 F. Supp. at 1019 (describing how Cyber Promotions responded to CompuServe's use of filtering software by modifying its messages to evade detection by CompuServe's software).

186. *See id.* at 1019-20 (addressing perpetuating temporary restraining order issued in early part of action).

187. *See id.* at 1020 (continuing temporary restraining order and examining CompuServe's motion for injunction, predicated on common law theory of trespass to chattels against Cyber Promotions's sending unsolicited advertisements to e-mail addresses of any of CompuServe's customers).

188. *See id.* at 1021 (canvassing Ohio case law and secondary sources to find that trespass to chattels is actionable tort in Ohio).

189. *See id.* (stating that other courts have held that computer-generated and disseminated electronic signals are sufficiently physically tangible to support action for trespass to chattels). The court cited *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468 (Ct. App. 1996), which applies the trespass theory to damages arising from a defendant's computer hacking. In *Washington v. Riley*, 846 P.2d 1365, 1373 (Wash. 1993), the court found that, under Washington law, computer hacking was the criminal offense of "computer trespass." In *Indiana v. McGraw*, 480 N.E.2d 552, 554 (Ind. 1985), the court recognized in dictum that a computer hacker's unauthorized access to a computer network was akin to trespass. Arguably, the *Riley* and *McGraw* cases are distinguishable from the *CompuServe* case because the first two involve criminal charges under state statutory law. *Riley*, 846 P.2d at 1368; *McGraw*, 480 N.E.2d at 552. However, these distinctions are not as important as the recognition by the Indiana and Washington courts that computer or electronic signals can give rise to causes of action, whether criminal or civil.

190. *See CompuServe*, 962 F. Supp. at 1022 (explaining that plaintiff can maintain action for trespass to chattels absent interference with right to possess chattel if it can show harm to personal property or diminution in property's value, quality, or condition as result of defendant's use). The court based its reasoning on the *Restatement (Second) of Torts* which lays out one of the circumstances under which a person who commits a trespass to chattel may be liable to the chattel's possessor. *Id.* at 1021-22; RESTATEMENT (SECOND) OF TORTS § 218(b) (1965). The *Restatement* states that "[t]here may . . . be situations in which the value to the owner of a particular type of chattel may be impaired by [the defendant's] dealing with it in a manner that does not affect its physical condition." *Id.* § 218 cmt. h.

an action for trespass to chattels must show intent and actual damages in order to proceed with the claim.[191]

To prove intent, a plaintiff can show that it gave the defendant actual notice that the defendant was not permitted on the plaintiff's property.[192] Because CompuServe explicitly told Cyber Promotions that Cyber Promotions did not have CompuServe's consent to use CompuServe's system, CompuServe could clearly prove intent.[193] Additionally, CompuServe obviated any defense based on consent because it never expressly granted Cyber Promotions the privilege to use CompuServe's resources.[194] Any initial consent Cyber Promotions may have had by virtue of CompuServe's connection to the Internet vanished, in the court's view, when CompuServe unequivocally told Cyber Promotions to stop using the CompuServe network.[195]

In assessing whether CompuServe had demonstrated actual damages sufficient to support a preliminary injunction, the court reasoned that CompuServe had succeeded in showing that potential actual damages arose from the

---

191. *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (explaining that tort of trespass to chattels requires some actual damage as prima facie element); *id.* at 1024 (stating that plaintiffs must prove that would-be trespasser acted with intent in order to prove liability for trespass).

192. *See id.* at 1024 (stating that plaintiffs can prove intent necessary to sustain action for trespass by demonstrating that plaintiff gave defendant actual notice that plaintiff would not permit defendant to use plaintiff's property). The court observed that CompuServe's use-policy expressly prohibits use of CompuServe's facilities for sending unsolicited e-mail messages. *Id.* Although the statement of this policy on the Internet might be insufficient notice to potential third-party users, the court stated that it was not concerned with that risk in this case. *Id.*

193. *See id.* (explaining that CompuServe employee specifically told owner of Cyber Promotions that it could not use any of CompuServe's equipment to send junk e-mail).

194. *See id.* at 1023-24 (explaining defense of privilege granted by owner of chattels and fact that CompuServe explicitly had denied any such privilege).

195. *See id.* (explaining that property owner can rescind consent to use by third party and that any use after recission is trespass and explaining that CompuServe did rescind any privilege that might have existed by virtue of CompuServe's connection to Internet). The court also addressed whether Cyber Promotions might have a special privilege to use CompuServe's system under common carrier or public utility theories. *Id.* at 1025. Although Cyber Promotions did not advance this argument, the court addressed and then dismissed such an argument. *Id.* To determine whether an entity is a public utility, the court engaged in a multi-step analysis. *Id.* First, the entity must devote a service or good to the use of the general public. *Id.* Second, the general public must also have a legal right to demand or to receive the service or good. *Id.* Last, a public utility must also conduct its business as a matter of public concern, such as a monopoly or oligopoly. *Id.* (citing A&B Refuse Disposers, Inc. v. Board of Ravenna Township Trustees, 596 N.E.2d 423, 425-26 (Ohio 1992)). *But see* Goldstone, *supra* note 84, at 40-47 (explaining how courts and regulators could apply general common carrier principles to ISPs and how applying those principles could help message senders); Note, *The Message in the Medium: The First Amendment on the Information Superhighway*, 107 HARV. L. REV. 1062, 1064-67 (1994) (suggesting ways in which computer networks are like common carriers).

drain that Cyber Promotions's large amount of e-mail put on CompuServe's computer disk space and power.[196] Because of the spamming, CompuServe's resources were not available to its subscribers.[197] As a result, CompuServe's business reputation and goodwill with customers suffered potential harm.[198] Based on the difficulty of quantifying CompuServe's harm, the court determined that a preliminary injunction was an appropriate interim measure to protect CompuServe from possible additional harm.[199]

In the court's final balancing between the harm to the plaintiff and the harm to the defendant, the court concluded that the harm to CompuServe outweighed any harm Cyber Promotions might suffer from the issuance of a preliminary injunction.[200] The court decided, as a matter of public policy, that it was best to protect the common-law rights of property owners.[201] The court found that if the defendant were to prevail on its First Amendment defense,[202] the resulting high volumes of junk e-mail would most likely harm the viability of e-mail as an effective communication system.[203]

In the *Thrifty-Tel* and *CompuServe* decisions, the courts present an interesting application of old law to a new situation.[204] However, by employing the

---

196. *See CompuServe*, 962 F. Supp. at 1022 (acknowledging CompuServe's affidavit stating that handling large volume of bulk e-mail had drained CompuServe computer resources and thus resulted in diminution of value of computer equipment).

197. *See id.* (stating that result of Cyber Promotions's e-mail messages was to make CompuServe's network unavailable to its customers).

198. *See id.* (stating that result of Cyber Promotions's bulk e-mail was to diminish available resources for CompuServe customers).

199. *See id.* at 1027-28 (stating that plaintiff had shown that defendant's intrusions into plaintiff's computer system resulted in harm to plaintiff's business reputation and goodwill which was intangible loss that preliminary injunction would mitigate).

200. *See id.* at 1028 (concluding that plaintiff would suffer irreparable harm without injunction and that defendant would not suffer because it could employ alternative means to disseminate its message).

201. *Id.*

202. *See id.* at 1025-27 (discussing defendant's attempt to use First Amendment as defense). The court rejected this argument on two grounds. First, the court observed that CompuServe was a private company and did not exercise any traditional state functions, and thus, it was not subject to First Amendment scrutiny. *Id.* at 1026-27. Second, the court stated that because Cyber Promotions's acts exceeded any consent that CompuServe granted, the First Amendment could not provide Cyber Promotions a defense. *Id.* at 1027.

203. *Id.* at 1028. In determining that the harm to the defendant was not significant, the court stated that "[h]igh volumes of junk e-mail devour computer processing and storage capacity, slow down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel, and cause recipients to spend time and money wading through messages that they do not want." *Id.* The court also observed that if customers of CompuServe do not like this order, the customers can choose another ISP that accepts spam. *Id.*

204. *See* Bennett, *supra* note 141, at 560-63 (addressing definition of trespass to chattels in cyberspace); Hawley, *supra* note 141, at 392-96 (commenting on use of trespass to chattels

trespass to chattels theory, the courts limited the possibility that the owner of a private computer or e-mail system can protect itself from trespasses to its property.[205] The question remains whether these cases present a new paradigm by which to judge all cases involving unsolicited e-mail or whether the *Thrifty-Tel* and *CompuServe* cases are limited to their facts. The *Intel* case provides an interesting context in which to analyze these issues.

### *V. Protecting Private Network Providers from Unwanted E-Mail*

Although the *Intel* case and the commercial ISP cases appear similar, the cases implicate different issues with respect to the harm to the plaintiffs' property interests.[206] The factual distinctions make it apparent that trespass to chattels will not adequately protect Intel's interest in its private network.[207] Trespass to chattels requires that a plaintiff prove that it has suffered tangible harm.[208] It may be difficult for a private network provider to prove it has suffered tangible harm while it is still suffering intangible harm.[209] Thus, if Intel and other private network providers are to protect their interests, they will need to find another theory.[210] A limited expansion of the protections afforded in cases of trespass to real property will most effectively protect a private network provider's interest because the private network provider may obtain relief when the harm is merely nominal.[211] The following subparts detail the limitations of the trespass to chattels theory and the alternative limited analogy to trespass to real property.[212]

---

to protect ISPs' and consumers' interests). *See generally* Mark D. Robins, *Electronic Trespass: An Old Theory in a New Context*, 15 No. 7 COMPUTER LAW. 1 (1998) (discussing application of old common law theory to electronic contacts resulting in trespass to chattels)

205. *Compare* RESTATEMENT (SECOND) TORTS § 158 (1965) (holding actor liable for trespass irrespective of harm to land of another) *with* RESTATEMENT (SECOND) TORTS § 218(b)-(c) & cmt. e (1965) (stating that actor is liable for trespass to chattels only if trespass results in actual harm).

206. *See infra* Part V.B (distinguishing harm to Intel from harm to ISPs).

207. *See infra* Part V.A-B (explaining *Intel* facts and how trespass to chattels will not adequately protect interests).

208. *See supra* notes 154-59 and accompanying text (explaining tangibility requirement for succeeding on trespass to chattels claim).

209. *See infra* notes 246-53 (providing examples of intangible harm that private network providers might suffer if unable to stem tide of unsolicited e-mail).

210. *See infra* Part V.B-C (suggesting that alternative theory to trespass to chattels is necessary).

211. *See infra* Part V.C (discussing use of limited trespass to land claims to protect private network provider's interests).

212. *See infra* Part V.A-C (detailing why trespass to chattels is insufficient to protect private network providers and explaining how and why limiting trespass to real property would provide effective remedy for trespass to computer networks).

### *A. Factual Background of* Intel v. Hamidi

As discussed in Part I, a former employee of computer-chip giant Intel has used a Web page and e-mail to spread his message condemning Intel's employment practices.[213] In response to perceived abuses by Intel against its employees, a former Intel employee, Ken Hamidi, and other former Intel employees created a group named AXEI, now named FACE Intel.[214] Hamidi, the group's spokesperson and contact, states that the group's primary purpose is to challenge Intel's personnel policies and to promote long-term employment possibilities at Intel.[215] FACE Intel spreads its message of opposition to Intel's personnel policies through its Web site and by sending mass e-mail messages to current Intel employees.[216]

FACE Intel sent its first mass e-mail to Intel employees in December 1996, with follow-up e-mail messages in March and April of 1997.[217] The group sent more e-mail in February and March of 1998.[218] In spring 1998, Intel asked Hamidi and FACE Intel to return its list of Intel employee e-mail addresses and demanded that Hamidi cease and desist from sending any additional e-mail over the Intel computer system, including the company e-mail system.[219] Responding to Intel's request, Hamidi claimed that he and other

---

213. *See supra* Part I (discussing background giving rise to *Intel v. Hamidi*).

214. *See* Complaint, *supra* note 9 (explaining origins of FACE Intel); Intel's Motion for Summary Judgment, *supra* note 8, at 1 (explaining background on source of e-mail from FACE Intel); *see also FACE Intel* (visited Jan. 14, 2000) <http://www.faceintel.com/whoweare.htm> (explaining acronym, purpose of group, and setting forth FACE Intel's grievances against company). The acronym FACE Intel stands for Former and Current Employees of Intel. *Id.* Specifically, FACE Intel claims that Intel engages in age discrimination, medical disability discrimination, and race and ancestry discrimination. *Id.* Further, FACE Intel takes issue with the termination procedures that Intel follows. *Id.* Hamidi himself is a former employee who lost his position after a protracted battle over disability benefits. *See* Rita Ciolli, *Web as Weapon: Victims of Online Attacks Seek Limits for New Medium*, NEWSDAY, Feb. 15, 1999, at A5 (providing background on Hamidi's dispute with Intel).

215. *See FACE Intel* (visited Jan. 14, 2000) <http://www.faceintel.com/whoweare.htm> ("FACE Intel Group Mission: To influence positive human resources policies and practices and create true long-term employment opportunities at Intel"); *see also* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (stating that Hamidi has identified himself as officer and designated spokesman for FACE Intel).

216. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (explaining what activities FACE Intel engages in to spread its message).

217. *Id.*

218. *Id.*

219. *See* Letter from Morrison & Foerster, Intel's attorneys, to Ken Hamidi and FACE Intel 1-2 (Mar. 17, 1998) (located at *Intel v. Hamidi* (visited Jan. 14, 2000) <http://www.Intelhamidi.com/intelletters.htm>) [hereinafter Morrison Letter] (telling Hamidi, as FACE Intel contact person, that FACE Intel illegally was using Intel employee addresses and that FACE Intel was trespassing on Intel's proprietary computer system, and that if FACE Intel did not stop

members of FACE Intel had compiled the employee lists from their own labor, and thus the lists were not property of Intel.[220] Hamidi further asserted that the First Amendment protects the transmission of e-mail over the Internet.[221] Despite Intel's request, Hamidi did not stop; rather, he sent another bulk e-mail in September 1998.[222]

After Hamidi's refusal to comply with Intel's request, Intel filed suit on October 7, 1998 in Sacramento Superior Court against Kenneth Hamidi and FACE Intel, alleging trespass to chattels and nuisance.[223] On November 27, 1998, the California Superior Court granted Intel a preliminary injunction.[224] The order prohibited Hamidi from sending any further e-mail to Intel employees over Intel's computer network.[225] On June 17, 1999, the court entered a permanent injunction in favor of Intel;[226] the question that arises now is whether the court properly based its decision on trespass to chattels or if the court should have found a slightly different basis for the ruling.[227] Intel then

---

immediately, Intel would take court action). Intel has dropped any claims with respect to the employee lists. *Compare* Morrison Letter, *supra*, at 1 (stating that employees lists are property of Intel) *with* Complaint, *supra* note 9 (making no mention of employee lists).

220. *See* Letter from Ken Hamidi, FACE Intel Spokesperson, to Linda E. Shostak, Morrison & Foerster, Intel's attorneys 1 (Jan. 14, 2000) (located at *Intel v. Hamidi* (visited Oct. 28, 1999) <http://www.Intelhamidi.com/intelletters.htm>) [hereinafter Hamidi's Letter] (arguing that lists cannot be proprietary information of Intel because FACE Intel members compiled the lists with their own labor).

221. *See* Hamidi's Letter, *supra* note 220, at 1 (stating that sending e-mail is merely use of Internet to exercise free speech rights).

222. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (detailing events leading to filing of complaint against Hamidi and FACE Intel); *see also Intel v. Hamidi* (visited Jan. 14, 2000) <http://www.Intelhamidi.com/septembermail.htm> (containing text of FACE Intel September e-mail).

223. Complaint, *supra* note 9, at ¶¶ 4-12, 14-15.

224. *See* Preliminary Injunction, *supra* note 17 (granting preliminary injunction until final judgment after trial on merits). Although this Note argues that a limited application of trespass to real property provides a better basis for a permanent injunction than does a trespass to chattels claim, it is not unreasonable that the court granted the preliminary and permanent injunctions on the basis of the trespass to chattels theory. The ISP cases and the *Intel* case are sufficiently analogous that upon first viewing they appear identical. However, after further examination of the factual distinctions, it becomes apparent that the Intel case and the ISP cases are distinguishable such that a different theory should have been necessary for Intel to prevail. *See infra* Part V.B (distinguishing *Intel* facts from facts of cases in which ISPs won on trespass to chattels claims).

225. *See* Preliminary Injunction, *supra* note 17 (prohibiting Hamidi or FACE Intel from sending any unsolicited e-mail or from otherwise using or accessing Intel's computer system).

226. *See* Order for Entry of Final Judgment, Intel Corp. v. Hamidi, No. 98AS05067 (Sacramento Super. Ct. June 16, 1999) (stating that court issued injunction in favor of Intel on June 16, 1999), *available at* <http://www.intelhamidi.com/permanentinjunction.htm#Order for entry of final judgment>.

227. *See infra* Part V.B-C (analyzing Intel's trespass to chattels claim and suggesting

won a permanent injunction against Hamidi and FACE Intel on the basis of trespass to chattels. This Note argues that trespass to chattels is neither the most accurate nor the most effective basis for this injunction.[228]

### *B. Intel's Arguments: How Trespass to Chattels Fails to Protect the Private Network Provider's Interests*

To win summary judgment on the trespass to chattels claim, Intel alleged, relying on *Thrifty-Tel* and *CompuServe*,[229] that Hamidi and FACE Intel trespassed on Intel's proprietary computer system by sending unauthorized and unwelcome e-mail to addresses on the system.[230] These cases support the

---

alternative theory of recovery). Hamidi also has suggested in several places that he believes that the First Amendment protects his right to send e-mail to Intel over their system, and thus, an injunction would be impermissible. *See* Hamidi's Letter, *supra* note 220, at 1; Ken Hamidi, *Intel v. Hamidi* (visited Jan. 14, 2000) <http://www.Intelhamidi.com/casedocuments.htm> (explaining that Hamidi regards lawsuit as question of protecting First Amendment right of free speech). This defense did not prevail at the superior court level. Arguably, those who send a large amount of unsolicited e-mail could claim First Amendment protection based either on the public forum doctrine or on the state action doctrine. However, a discussion of the First Amendment is beyond the scope of this Note. Various commentators have addressed First Amendment issues with respect to the Internet. *See generally* JONATHAN W. EMORD, FREEDOM, TECHNOLOGY AND THE FIRST AMENDMENT (1991); Goldstone, *supra* note 84 (discussing application of public forum doctrine in cyberspace); Allen S. Hammond, *Private Networks, Public Speech: Constitutional Speech Dimensions of Access to Private Networks*, 55 U. PITT. L. REV. 1085 (1994); Cass R. Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757 (1995) (addressing effect of First Amendment on Internet regulation issues); Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995) (discussing effect of Internet on free speech of marginal groups in society). For a discussion of the possible state action argument that Hamidi could make to protect his acts, see Development: III, *supra* note 96, at 1622-34.

228. *See infra* Part V.B-C (distinguishing *Intel* from other ISP cases and arguing that distinction makes trespass to chattels inapposite).

229. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 3 (analogizing reasoning in *Thrifty-Tel* and *CompuServe* to support argument that Hamidi's sending e-mail to e-mail addresses on Intel's network constituted trespass to chattels); *supra* Part IV.C-D (discussing *Thrifty-Tel* and *CompuServe* cases).

230. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 1-3 (arguing that under California law, access to proprietary computer system without consent constitutes trespass to chattels). Intel did not address its nuisance count in its motion for summary judgment. *Compare* Complaint, *supra* note 9, at ¶¶ 14-15 (alleging nuisance) *with* Intel's Motion for Summary Judgment, *supra* note 8, at 2-4 (failing to address nuisance claim). Nuisance is an action to recover for a nontrespassory invasion of a possessor's private use and enjoyment of land. RESTATEMENT (SECOND) TORTS § 821D (1965). In a case of invasion of a private network, employing a nuisance theory would require an extension of the notions of real property. This Note does argue for extending the notions of property in order to allow the same protection for network trespasses that land trespasses receive. *See infra* Part V.C. However, even if courts extend real property notions, the specific theory of nuisance will not protect the private network provider as well as trespass to land will protect the private network provider. To succeed on a

notion that use of another's computer system can constitute a trespass to chattels, but are distinguishable from the *Intel* case.[231]

Analyzing *Intel* under a trespass to chattels theory demonstrates that Intel should not have been able to prove the actual harm requirement for relief, and thus, Intel should have failed in its trespass to chattels claim against Hamidi.[232] To succeed on trespass to chattels, Intel first had to establish that Hamidi had in fact intermeddled with the chattel.[233] Intel could demonstrate the physical contact requirement of intermeddling because Hamidi's contact with Intel's computer system was via e-mail, and courts already have established that electronic signals are sufficiently tangible to support an action for trespass.[234] Intel could prove the next key requirement, the intent to intermeddle with the property in question, through Hamidi's own admissions.[235] For example, in his letter responding to Intel's demand to cease sending any e-mail over the Intel computer network, Hamidi said that in sending the e-mail, he was exercising his "free speech rights . . . on the Internet."[236] Furthermore, Intel's notice to Hamidi that Intel no longer would allow him to send e-mail on the Intel system revoked any implied consent to use the Intel system that arises from Intel's connection to the Internet.[237]

---

nuisance claim, the plaintiff would have to show that the intentional acts of the defendant were unreasonable. RESTATEMENT (SECOND) TORTS § 822(a) (1965). To be unreasonable, the defendant's acts must cause grave harm that outweighs the utility of the defendant's acts, or the defendant's acts must cause harm that is serious, monetarily compensable and compensability would not make continuation of the defendant's acts unfeasible. *Id.* § 826. Trespass, in contrast, does not require a showing of such grave harm because it protects the possessor's interest in the inviolability of the land in question; thus, any entry upon the land could subject an actor to liability. *Id.* § 821D cmt. d. In the context of the invasion of an interest in a computer network, nuisance would not permit recovery when the plaintiff could not show serious harm. *Id.* §§ 822, 826; *see also supra* Part IV.C (explaining necessity of showing harm in action for trespass to chattels).

231. *See infra* notes 222-37 and accompanying text (distinguishing ISP cases from *Intel* case).

232. *See* RESTATEMENT (SECOND) TORTS § 218 cmt. e (1965) (requiring showing of actual harm to recover for trespass to chattels).

233. *See supra* Part IV.B (discussing elements of trespass to chattels).

234. *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (stating that electronic signals from computers are sufficient to support action for trespass to chattels); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 n.6 (Ct. App. 1996) (same); *supra* Part IV.C-D (developing use of trespass to chattels in electronic context).

235. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (stating that Hamidi has admitted to at least three of mass e-mail messages that Intel has received); *see also* Hamidi's Letter, *supra* note 220, at 1 (denying that e-mail constituted spam or that FACE Intel or Hamidi has trespassed on Intel's property).

236. Hamidi's Letter, *supra* note 220, at 1.

237. *See* Morrison Letter, *supra* note 219, at 1 (telling Hamidi to cease and desist from sending any further e-mail on Intel e-mail system); Intel's Motion for Summary Judgment,

Finally, Intel needed to prove that Hamidi's e-mail contact with Intel's computers caused actual harm in order to succeed on a trespass to chattels claim.[238] However, Intel did not allege any specific harm that Hamidi's e-mail trespasses caused.[239] Intel alleged neither physical harm to the chattel nor impairment to the value of the chattel.[240] Instead, Intel attempted to analogize its harm to the harm that CompuServe suffered at the hands of Cyber Promotions: damage to its goodwill and business reputation.[241] However, Intel failed to explain how Hamidi's e-mail harmed Intel's business in the same way that Cyber Promotions's e-mail damaged CompuServe's business.[242] As the court in *CompuServe* explained, CompuServe derives value from its network, wholly to the extent that CompuServe's computer equipment can serve the subscriber base.[243] Intel did not show that Hamidi's e-mail drained Intel's computer resources so as to deprive paying customers of access to a service that Intel offers.[244] Furthermore, because Intel does not offer e-mail or network services to outside parties, it could not have suffered loss of goodwill from customers

---

*supra* note 8, at 1 (referencing letter, from lawyers, informing Hamidi that Intel expressly prohibited Hamidi from sending e-mail to Intel).

238. *See supra* notes 154-59 and accompanying text (discussing requirement of showing of actual damages in order to find actor liable for trespass to chattels).

239. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 1-5. At no point in its Motion for Summary Judgment does Intel explain what actual damages it has suffered because of Hamidi's e-mail messages. *Id.*

240. *See* RESTATEMENT (SECOND) TORTS § 218 cmt. h (1965) (commenting that harm to chattel may be physical harm or dealing with chattel so as to impair its value, irrespective of actual physical harm). The *Restatement* uses the example of a toothbrush. *Id.* If an actor uses the toothbrush of another, the actor's use has not physically destroyed or damaged the toothbrush. *Id.* However, the owner may not want to use the toothbrush again, and thus, the actor's use has rendered the toothbrush virtually useless to the owner. *Id.*

241. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 2-3 (citing to harm that CompuServe suffered as result of spam sent over its system). Intel does not support its implication of equivalent harm with similar evidence of the equivalent harm. In *CompuServe*, the ISP could demonstrate that customers had threatened to discontinue service and that the volume of spam had significantly affected the availability of service to the ISP's customers. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019, 1022, 1027-28 (S.D. Ohio 1997). Thus, the court determined that CompuServe had suffered harm to its goodwill and reputation. *Id.* at 1021-22.

242. *Compare* Intel's Motion for Summary Judgment, *supra* note 8, at 1-3 (referencing CompuServe's harm but failing to comment upon actual harm that Intel suffered) *with CompuServe*, 962 F. Supp. at 1022-23 (explaining harm that CompuServe has suffered to its business reputation and goodwill as result of Cyber Promotions's e-mail messages).

243. *See CompuServe*, 962 F. Supp. at 1022 (explaining source of value for CompuServe's computer systems).

244. *See id.* at 1022-23 (explaining that Cyber Promotions's e-mail harmed business reputation and goodwill by depriving CompuServe's customers of use of CompuServe's service).

who are paying for its service.[245] Although Hamidi successfully contacted approximately 29,000 Intel employees, this number does not compare to the millions of e-mail messages that spammers have sent to ISPs' subscribers.[246] Ultimately, failure to allege or to support a showing of actual harm should have precluded Intel from prevailing on a trespass to chattels theory.[247]

Although the court should have found that Intel lacked sufficient evidence to succeed on a trespass to chattels theory, this lack of evidence does not reflect an absence of harm to Intel. Hamidi's continuing e-mail intruded upon Intel's network and affected other interests that Intel has in its network. As information and its transmission have become economically more valuable,[248] private individuals and corporate entities have pursued their own interests in appropriating the value of information to their own use.[249] Such appropriations of value include, but are not limited to, the creation of the physical computer networks and Internet connections.[250] Intel is certainly no exception. Intel's network serves its corporate purposes by providing its employees a medium by which to work more efficiently, researching and communicating more rapidly.[251] Furthermore, Intel has exercised exclusive

245. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 4 (stating that Intel e-mail system is not open to use by members of general public and that Intel limits employees' personal use).

246. *Compare* Intel's Motion for Summary Judgment, *supra* note 8, at 2 (stating that Hamidi's most recent e-mail reached approximately 29,000 employees), *with* America Online, Inc. v. IMS, Inc., 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (stating that defendant had sent over 60 million pieces of unsolicited bulk e-mail over 10-month period), *and* Cyber Promotions, Inc. v. American Online, Inc., 948 F. Supp. 436, 438 (E.D. Pa. 1996) (stating that Internet advertiser had been sending literally millions of e-mail messages to ISP's customers).

247. *See supra* notes 154-59 and accompanying text (explaining that plaintiff must prove that it has suffered actual harm in order to recover for trespass to chattels). Even though Intel prevailed on the trespass to chattels claim, it is not certain that every private network provider will be able to do so, without rendering meaningless the harm requirement for trespass to chattels. Thus, an alternative theory of recovery still will be important.

248. *See supra* notes 1-3 and accompanying text (discussing value of information).

249. *See* McGinnis, *supra* note 2, at 102 (explaining that exercise of private property rights of private individuals and corporate entities has propelled growth of "transmission links" and Internet). For example, ISPs can survive economically because of the increased value that society places on the information available through their services. *Id.* Corporate America also has demonstrated its belief that telecommunications technology is a necessary element of doing business. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1223 n.122 (1998) (stating that American corporations have invested more than 50 billion dollars annually in telecommunications infrastructure).

250. *See* McGinnis, *supra* note 2, at 102 (stating that universities have provided employees with Internet links with hope that university ultimately will derive benefit from employees' use of Internet).

251. *See* ACLU I, 929 F. Supp. 824, 832-33 (E.D. Pa. 1996) (stating that employers often provide Internet connections to facilitate research and development); *see also* McGinnis,

control over the establishment of use policies, evidencing a clear intent to manage the network resource as its private property.[252] Additionally, Intel has an important interest in managing more than the physical use of the system, and thus, Intel defines and limits the use of the network and the permissible content of e-mails.[253] The trespass to chattels theory recognizes and protects a property interest in the physical functioning of the network.[254] However, a private network provider's interest in its network is broader than an interest merely in the network's physical value. Thus, it will be more difficult to quantify harm in order to prove the actual harm requirement for success on a trespass to chattels claim. An analogy to trespass to real property, in order to use the remedies available thereunder, will better protect the broader interest that a private network provider has in its network because the network provider will not need to prove actual harm.[255]

### *C. A Possible Solution for Private Network Providers*

Absent actual harm, the trespass to chattels theory fails to and should not be found to provide sufficient recourse for the private network provider that wants to rid itself of hostile or unsolicited e-mail.[256] If a private network

---

*supra* note 2, at 102 (suggesting that employers obtain benefits of employee connection to Internet and e-mail); Stephanie Stahl, *Dangerous E-mail*, INFO. WEEK, Sept. 12, 1994, at 12 (explaining that employers provide access to Internet and e-mail for employees to reduce number of telephone calls, paper memos, and face-to-face meetings). Obviously, Intel's corporate purposes would not include providing its critics with a forum to express that criticism to current Intel employees.

252. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 2 (stating that Intel has established use policies for its computer network); *see also* 2 WILLIAM BLACKSTONE, COMMENTARIES 2 (1957) (commenting that nothing causes more debate than right of property); Anthony M. Honore, *Ownership*, *in* OXFORD ESSAYS IN JURISPRUDENCE, 107, 108-124 (A. Guest ed., 1967) (expressing right to manage as one of rights of ownership of property). In his inimitable words, Blackstone defines the right of property as "that sole and despotic dominion which one [person] claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe." BLACKSTONE, *supra*, at 2.

253. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 2 (stating that Intel has established use policies for its computer network); Meyerson, *supra* note 2, at 140-41 (suggesting that network owners have right to define use of network); Jarrod J. White, *E-mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1079-80 (1997) (recognizing that employers have interest in monitoring employee e-mail in order to protect against liability and poor productivity).

254. *See* America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 552 (E.D. Va. 1998) (granting injunction for trespass to chattels); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1028 (S.D. Ohio 1997) (same).

255. *See infra* Part V.C (applying trespass to land theory to network trespass).

256. *See supra* notes 154-59 and accompanying text (explaining that plaintiff cannot recover for nominal harm in trespass to chattels actions); *see also supra* Part V.B (explaining that private network provider may not be able to demonstrate actual harm).

provider, such as an employer, determines that it does not want to continue receiving unsolicited bulk e-mail, it has several options. First, it may attempt to prevent delivery of the spammer's e-mails by employing filtering devices.[257] Next, it can demand that the spammer cease and desist.[258] After exhausting these self-help methods, seeking judicial help is the only other recourse.[259] Trespass to chattels provides one legal theory with which to attack spammers.[260] However, as discussed above, if the trespass to chattels theory is imperfect, it may fail to protect the private network provider's broader interests in its network.[261] A trespass to real property theory may provide the protection that a trespass to chattels theory does not.[262] Analogizing the private network provider's interests to a real property interest would permit the provider to hold a spammer liable for trespass without necessitating a demonstration of actual harm.[263]

---

257. *See CompuServe*, 962 F. Supp. at 1023 (stating that court expects plaintiffs to use technological self-help measures before resorting to courts to solve spamming issues); Carroll, *supra* note 86, at 255-56 (explaining that numerous self-help or "vigilante" mechanisms exist for ridding Internet of persistent spammers). Carroll also explains that ISPs attempt to control spam both by filtering e-mail with software applications and by establishing use agreements that make spamming by ISP account holders grounds for terminating the service contract. *Id.* at 256-57.

258. *See America Online*, 24 F. Supp. 2d at 549 (stating that plaintiff ISP had demanded that defendant spammer cease sending e-mails over plaintiff's network); *CompuServe*, 962 F. Supp. at 1019, 1024 (same).

259. *See* Sorkin, *supra* note 138, at 1024-27 (discussing inadequacy of most self-help measures because they allow unwanted messages to slip through and filtering devices often do not prevent unwanted e-mails from consuming network resources); Hawley, *supra* note 141, at 411-16 (discussing self-help measures to reduce incidence of spamming and observing that some efforts are not wholly effective). One problem with filtering, for example, is that it might filter out desirable e-mail in addition to the unwanted e-mail. *Id.* at 415-16.

260. *See supra* Part IV.B-D (setting forth use of trespass to chattels to combat spam).

261. *See supra* notes 237-45 and accompanying text (discussing inadequacy of trespass to chattels theory in context of private network provider because of interest in network that is broader than interest in mere chattel value).

262. *See infra* notes 263-82 (discussing application of trespass to real property theory to protect private network provider's interests).

263. *See* RESTATEMENT (SECOND) OF TORTS § 158(a) (1965) (stating that trespasser may be liable for trespass even if trespasser causes no actual harm to property). Although conversion might also appear to be a possible action to recover for an interference with possession, conversion will not work in the network trespass cases. The primary distinction between trespass to chattels and conversion is in the measure of damages. *Id.* § 222A cmt. c. In conversion, the plaintiff recovers the full value of the chattel. *Id.* However, a plaintiff can recover only for the value of the harm in an action for trespass to chattels. *Id.* Thus, to recover in an action for conversion, the plaintiff must show that the actor's exercise of dominion or control over the plaintiff's chattel constituted such a serious and substantial interference with the plaintiff's right to possession that the plaintiff should recover the chattel's full value. *Id.* Furthermore, conver-

Under a traditional trespass to real property theory, an actor may be liable for trespass in several situations.[264] An actor will be liable for trespass if the actor intentionally enters land or causes a thing to enter land that is in the possession of another.[265] An actor also will be liable for trespass if the actor intentionally remains on the land in the possession of another after the possessor has informed the actor that the actor does not have consent to be on the land.[266] In either situation, the actor will be liable regardless of whether the actor caused or intended to cause actual harm to the property.[267] To prove the actor's intent to enter or remain on the land, the possessor of the land need only demonstrate that the actor meant to be present on the land in question;[268] the possessor of the land does not have to show that the actor intended any harm to the land.[269] Furthermore, even if the actor mistakenly believes either that the owner has consented to the actor's entering the land or that a privilege protects the actor's entry, the actor will be liable for trespass.[270] Moreover, if the owner has consented to the actor's presence on the land, but has since revoked that consent, then the actor will be liable for any further or continuing

---

sion's tangibility requirement will preclude recovery when the harm affects an intangible interest. *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 15, at 90-92 (5th ed. 1984) (explaining tangibility requirement of conversion). Thus, conversion does not protect intangible interests such as a private network provider might have in controlling the content that flows to its network. *Id.*; *see also* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 472-73 (Ct. App. 1996) (discussing cases that rejected use of conversion when harm was to intangible interests).

264. *See* RESTATEMENT (SECOND) OF TORTS § 158 (1965) (setting forth situations in which actor will be liable for any intentional intrusion on land).

265. *See id.* § 158(a) (stating that liability for trespass arises if actor enters land intentionally or causes something to enter land). The *Restatement* uses the example of a sand pile next to the property boundary line. If the actor piles a sand pile in such a way that the sand slides onto the neighbor's land, then the actor has committed a trespass. *Id.* § 158 cmt. e.

266. *Id.* § 158(b) (explaining that actor is subject to liability for intentionally remaining on land that is in possession of another).

267. *Id.* § 163 & cmt. b (explaining liability to possessor for trespass on land even if presence on land causes no harm to property interest of possessor). Merely acting under the certainty that one's acts will result in presence on the land will result in liability. *Id.* § 163 cmt. c.

268. *See id.* § 163 cmt. b (explaining that intention necessary to make actor liable for trespass is intention to enter land in question).

269. *See id.* (explaining that intent means intent to be present on land, not intent to cause harm). The actor only must have the intent to be on the land, but the intruder does not have to have the intent to invade the owner's interest in the exclusive possession of the land. *Id.*

270. *See id.* § 164 (stating that mistake as to consent or privilege does not relieve actor from liability for trespass). The *Restatement* states that mistake as to law or fact will not relieve the actor of liability for being present on another's land. *Id.* § 164 cmts. d-e. However, the *Restatement* states that if the possessor has induced the actor's belief, then the actor will not be liable for trespass. *Id.* § 164 cmt. b.

entries onto the land.[271] In the context of a trespass to a private computer network, the most important aspect of an action for trespass to lands is that the provider would be able to recover without needing to prove actual harm.[272]

Analyzing the *Intel* case under the trespass to land theory demonstrates how the theory applies to protecting the private network provider's interest.[273] To succeed, Intel first would have had to demonstrate that Hamidi intentionally entered or remained on Intel's property, which is Intel's computer network in this case.[274] Although Hamidi did not enter Intel's network himself, he caused electronic signals to enter the network by sending e-mails to up to 29,000 Intel employees at their Intel e-mail addresses.[275] Intel can prove Hamidi's intent to enter the property by Hamidi's own admissions.[276] Furthermore, Hamidi has made clear that sending e-mails directly to Intel employees is one of the methods he and FACE Intel used to attempt to influence Intel employment policies.[277]

---

271. *See id.* § 171(b) (explaining that property owner can revoke consent for actor to be on land).

272. *Id.* §§ 163, 164 cmt. a. Both of these sections indicate that liability for trespass to land will arise regardless of the actor's causing harm to the land or its value. *Id.* The actor's mere presence on the land will suffice to confer liability. *Id.*

273. *See supra* Part V.A (discussing facts of *Intel* case).

274. *See* RESTATEMENT (SECOND) TORTS § 158 (1965) (requiring intentional entry to or remaining on land). Obviously, this analysis assumes that the network provider has an interest greater than a chattel interest in the network. *See supra* notes 237-45 and accompanying text (examining private network provider's interest). As this Note has discussed, the courts already have recognized that network providers have a property interest in their networks, as chattel. *See supra* Part IV.C-D (discussing application of trespass to chattels theory to trespasses to computer networks). Although a network is not land in the traditional sense of a plot of earth, the network provider does have an interest in protecting the network from nonconsensual invasions. *See supra* notes 237-45 and accompanying text (discussing property interest in computer networks).

275. *See* RESTATEMENT (SECOND) TORTS § 158 cmt. i (1965) (explaining that actor will be liable for trespass if actor sends or causes something to enter land in possession of another or if actor knows that act, to substantial certainty, will result in entry onto property); *see also* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (stating that electronic signals from computers are sufficiently physical to support action for trespass to chattels); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 n.6 (Ct. App. 1996) (same); Intel's Motion for Summary Judgment, *supra* note 8, at 2 (stating that Hamidi's most recent e-mail reached approximately 29,000 employees).

276. *See* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (stating that Hamidi has admitted to at least three mass e-mailings that Intel has received); *see also* Hamidi's Letter, *supra* note 220, at 1 (denying that e-mails constitute spam or that FACE Intel or Hamidi has trespassed on Intel's property); *supra* notes 225-27 and accompanying text (discussing Intel's proving Hamidi's intent to have his e-mails reach Intel's computer network).

277. *See FACE Intel* (visited Jan. 14, 2000) <http://www.faceintel.com/whoweare.htm> ("FACE Intel Group Mission: To influence positive human resources policies and practices and

A possessor may have consented to the actor's entry on the property.[278] However, the possessor can revoke the consent, thus subjecting the actor to liability for any further entries onto the possessor's land.[279] Hamidi has argued that Intel's connection to the Internet constitutes implied consent to use the Intel network to e-mail Intel employees.[280] Assuming implied consent existed, Intel expressly revoked its consent to Hamidi's using the Intel e-mail system.[281] Thus, Intel could have proved a trespass by demonstrating that Hamidi continued to send e-mails over the Intel network after Intel revoked its implied consent.[282] Last, unlike trespass to chattels, Intel would not have needed to demonstrate that Hamidi's e-mails have caused actual harm to Intel or its computer network.[283] Thus, suing under a trespass to land theory would more easily provide Intel, or a similar private network provider, with relief.[284]

For the trespass to land analogy to be reasonable, the courts should limit its applicability to cases in which the private network provider has expressly revoked consent to access the private network.[285] Connecting to the Internet seems to indicate a willingness to engage in information exchange through e-mail or through the Web.[286] If courts were then to say that any electronic

---

create true long-term employment opportunities at Intel"); *see also* Intel's Motion for Summary Judgment, *supra* note 8, at 1 (explaining that FACE Intel maintains Web page and sends e-mails to current Intel employees to spread its message).

278. *See* RESTATEMENT (SECOND) TORTS § 167 (1965) (explaining that possessor can grant consent to actor to enter land).

279. *See id.* § 171(b) (stating that if possessor revokes consent then actor will be liable for any further or continuing entries to property).

280. *See* Ken Hamidi, *FACE Intel* (visited Mar. 7, 1999) <http://www.faceintel.com/intelvhamidi.htm> (explaining Hamidi's position with regard to lawsuit).

281. *See* Morrison Letter, *supra* note 219, at 1 (informing Hamidi that Hamidi was to cease and desist from sending any more e-mails over Intel's network). There is little doubt that Hamidi received notice that Intel was revoking its consent. *See* Hamidi's Letter, *supra* note 220, at 1 (indicating that Hamidi had received letter informing him that Intel had revoked any implied consent to use its network to e-mail its employees).

282. *See* RESTATEMENT (SECOND) TORTS § 171(b) (1965) (stating that entries after revocation of consent will give rise to liability for trespass).

283. *Compare id.* § 218 cmt. e (stating that possessor must show actual harm in trespass to chattels action) *with id.* § 158(a) (stating that actor may be liable for trespass even if actor does not cause harm to land in trespass to land action).

284. *See supra* notes 228-37 and accompanying text (explaining Intel's difficulty with showing harm); *see also* RESTATEMENT (SECOND) TORTS § 158(a) (1965) (stating that actor may be liable for trespass, even absent showing of actual harm).

285. *See* RESTATEMENT (SECOND) TORTS § 171(b) (1965) (permitting possessor to revoke consent to enter land).

286. *See supra* Part II.A-C (discussing use of Internet, including e-mail and Web). Computer networking developed with the intention of facilitating information exchange. *See supra* notes 33-40 and accompanying text (explaining origins of Internet).

signal, such as e-mail, could give rise to an action for trespass, the result would be extreme: Every e-mail could subject an unwitting sender to liability for trespass.[287] Furthermore, such potential liability would go against the policy that the Supreme Court has set forth for judicial treatment of Internet issues.[288] The Court has indicated that courts and legislatures should minimize the constraints on Internet communication because of the Internet's broad democratizing character.[289] Thus, to be consistent with this policy, courts should limit the analogy between trespass to a network and trespass to land so that liability will arise only if the network provider has expressly revoked its consent.

Properly limited, the trespass to land analogy provides a logical means to protect private network providers' interests. The law commonly understands "property" to mean that bundle of legal rights, privileges, powers, and immunities that a person claims to something as against other persons.[290] Thus, property is more than a physical, tangible object or plot of land; property is a legally protectable interest.[291] The constituent interests can and will alter as new technologies arise.[292] As property notions change, courts already have begun to include computer networks in the list of property interests that the law should protect.[293] The very nature of the common law allows for the

---

287. *See* RESTATEMENT (SECOND) TORTS § 158 (1965) (subjecting trespasser to liability whether or not trespass causes harm); *id.* § 167 (stating that possessor can consent to actor's presence on land); *id.* § 171(b) (stating that if possessor revokes consent and actor has notice of revocation, then actor will be liable in trespass for any further entries to land).

288. *See* ACLU II, 521 U.S. 844, 868-70 (1997) (expressing appreciation for full value of Internet communications); *see also supra* Part III.A.2 (discussing *ACLU II*).

289. *See ACLU II*, 521 U.S. at 868-70 (embracing Internet technology as having broad democratic appeal and value); *see also* Kende, *supra* note 103, at 475 (commenting that Supreme Court may regard Internet as positive social force).

290. *See* Wesley N. Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16, 21-23 (1913) (discussing usage of term "property" and its meaning as physical thing, but more accurately as rights of owner in relation to something).

291. *See id.* (demonstrating that property is more conceptual and incorporeal than it is tangible thing).

292. *See* 1 RICHARD R. POWELL, POWELL ON REAL PROPERTY ¶ 13 (Patrick J. Rohan ed., 1998) (stating that new property rights arise whenever new technology or social changes reveal new scarcity). Powell gave several examples of creation of new property interests due to scarcity. *Id.* One example is the regulation of broadcast media because of limited frequencies for transmitting broadcasts. *Id.* Another example is the regulation of air space because of the increase in air traffic. *Id.*; *see* United States v. Causby, 328 U.S. 256, 265 (1946) (finding that courts should treat invasions of airspace as invasion of surface property). *See generally* Colin Cahoon, Comment, *Low Altitude Airspace: A Property Rights No-Man's Land*, 56 J. AIR L. & COM. 157 (1990) (discussing development of air-space property rights for land owners and discussing danger that addressing every overflight as trespass would hamper growth of air industry).

293. *See* America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 554 (E.D. Va. 1998) (granting

courts to adapt the "old" law of trespass to new and developing technology.[294] Courts should now expand the protections provided for by trespass to land to include trespasses to private networks.

## *VI. Conclusion*

Oliver Wendell Holmes once wrote: "To rest upon a formula is a slumber that, prolonged, means death."[295] To rest upon the notion that a private network provider has an interest only in the chattel value of its network would be a slumber that fails to appreciate the complexity of a private network provider's interest in its network. This Note addressed the inapplicability of the trespass to chattels theory to a situation in which a private network provider, an employer, wants to stop a flow of e-mails over its network.[296]

A network provider's interest in assuring the viability of its network extends beyond the network's mere functioning.[297] Although the trespass to chattels theory might provide some recovery for non-physical injuries, it does not permit the private network provider to protect itself from merely nominal harm.[298] Furthermore, trespass to chattels does not allow the private network provider to preempt actual harms that could arise from e-mail that comes from outside parties. Thus, in order to protect the private network provider's very real property interest in its network, the courts should allow a private network provider to proceed on a limited trespass to land theory.[299]

---

injunction for trespass to chattels); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1030 (S.D. Ohio 1997) (same); *see also supra* notes 238-45 (explaining private network provider's interest in network is broader than chattel interest); *cf.* McGinnis, *supra* note 2, at 103-04 (suggesting that those who create discussion groups on Internet have ownership interest in their created space). To support the suggestion that those creating discussion groups in cyberspace own the discussion group space, one commentator observes that the creators have the classic hallmark of ownership – the right to exclude others. *Id.*

294. *See* Rendleman, *supra* note 120, at 859 (stating that common law functions flexibly to respond to new issues and disputes); *see also* MELVIN ARON EISENBERG, THE NATURE OF THE COMMON LAW 154-161 (1988) (proposing generative conception of common law). Under Eisenberg's theory the common law "consists of the rules that would be generated at the present moment by application of the institutional principles of adjudication." *Id.* at 154.

295. *See* OLIVER WENDELL HOLMES, COLLECTED LEGAL PAPERS 306 (1920).

296. *See supra* Part V.B (discussing applicability of trespass to chattels to situations in which private network providers seek to stop flow of e-mails to their networks).

297. *See supra* notes 248-55 (explaining property interest of private network provider).

298. *See supra* Part V.B (explaining limits of trespass to chattels theory for protecting private network provider's interest).

299. *See supra* Part V.C (suggesting that analogizing to trespass to land would better protect private network provider's interest).