SANTA CLARA COMPUTER AND HIGH-TECHNOLOGY LAW JOURNAL

Volume 16

2000

SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL

CONTENTS

SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL

CONTENTS

CASE NOTES

SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL

SUBMISSION OF ARTICLES

The Editors of the *Journal* invite readers to submit articles of a legal, scholarly nature, with each fact and proposition appropriately footnoted. Articles and essays covering legal issues pertaining to intellectual property, patents, copyrights, trademarks, trade secrets, biotechnology, telecommunications, technology licensing, venture capital, antitrust, electronic commmerce, computer law, cyberspace law, and other current topics in high technology law are suitable for publication in the *Santa Clara Computer and High Technology Law Journal.*

Manuscripts should be submitted in duplicate, accompanied by a 3.5" disk copy in Microsoft Word and addressed to the Editor-in-Chief, *Santa Clara Computer and High Technology Law Journal*, Santa Clara University, School of Law, Santa Clara, California 95053. Alternatively, authors may submit manuscripts electronically by e-mailing them to chtlj-submissions@scu.edu. Authors with questions may call the *Journal* office at (408) 554-4197, communicate by fax at (408) 554-4191, or e-mail at chtlj@scu.edu.

Manuscripts should be double-spaced with one-inch margins. Manuscripts must contain appropriate footnotes. Citations must conform to *The Bluebook: A Uniform System of Citation* (16th ed. 1996). A title page with the author's name, address, telephone number, and professional background should also be submitted. Authors should keep a copy of their manuscript to facilitate editorial revisions. The *Journal* requires notification if any part of the manuscript has been previously published. Unless expressly requested by the submitting author and accompanied by a return envelope and postage, manuscripts will not be returned.

GENERAL INFORMATION

Subscriptions. The *Santa Clara Computer and High Technology Law Journal* is published twice a year by students of Santa Clara University School of Law, Santa Clara, CA, 95053. Subscriptions are $45 per year for domestic and $55 per year for international. Subscriptions are automatically renewed annually, unless notice of termination is received before expiration of a current subscription. Subscribers are requested to send change of address notification as soon as it is available. Please see our Subscription Information Page and Order Form to subscribe.

Reproduction of Articles. Except as otherwise expressly provided herein, the author of each essay, article, and comment in this issue has granted permission for copies of that work to be reproduced for classroom use in a nationally accredited law school, provided that: (1) copies are distributed at or below cost of reproduction; (2) the author and the *Journal* are identified; and (3) proper notice of copyright is affixed to each copy. The views expressed in this periodical are to be attributed to the authors and not to the *Santa Clara Computer and High Technology Law Journal*, its editors or Santa Clara University.

Citations. The text and citations contained in the *Journal* generally conform to *The Bluebook: A Uniform System of Citation* (16th ed. 1996), copyrighted by the Columbia Law Review Association, the Harvard Law Review Association, the *University of Pennsylvania Law Review*, and the *Yale Law Journal.*

Web Site. For more information about the publication, feel free to visit our web site – www.scu.edu/techlaw.

Cite as: SANTA CLARA COMPUTER & HIGH TECH. L.J.

ARTICLES

CYBER-CRIMES: A PRACTICAL APPROACH TO THE APPLICATION OF FEDERAL COMPUTER CRIME LAWS

Eric J. Sinrod[†] and William P. Reilly[††]

TABLE OF CONTENTS

[†] Eric J. Sinrod is a partner focusing on e-commerce issues in the San Francisco office of the national law firm Duane, Morris & Heckscher LLP. Mr. Sinrod can be reached at EJSinrod@duanemorris.com.

[††] William P. Reilly is a law student at the University of San Francisco and has a background in e-commerce and computer security. Mr. Reilly can be reached at WPReilly@duanemorris.com.

I. INTRODUCTION

Cyber-crime, once the domain of disaffected genius teenagers as portrayed in the movies "War Games" and "Hackers," has grown into a mature and sophisticated threat to the open nature of the Internet. "Cyber-criminals," like their non-virtual traditional criminal counterparts, seek opportunity and are attracted to vacuums in law enforcement. The news media is filled with reports of debilitating denial of service attacks, defaced web sites, and new computer viruses worming their way through the nation's computers. However, there are countless other cyber-crimes that are not made public due to private industry's reluctance to publicize its vulnerability and the government's concern for security.[1]

Along with the phenomenal growth of the Internet has come the growth of cyber-crime opportunities.[2] As a result of rapid adoption of

1. Michael Hatcher et al., *Computer Crimes*, 36 AM. CRIM. L. REV. 397, 399 (1999).

2. *See* Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839 (1999). In a recent survey of 643 computer security practitioners in the U.S., "[s]eventy percent reported a variety of serious computer security breaches other than the most common ones of computer viruses, laptop theft or employee 'net abuse' -- for example, theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks and sabotage of data or networks." Computer Security Insititute, *Ninety percent of survey respondents detect cyber attacks, 273 organizations report $265,589,940 in financial losses* (Mar. 22, 2000) <http://www.gocsi.com/prelea_000321.htm> [hereinafter CSI Survey]. The report also found that:

> Ninety percent of respondents (primarily large corporations and government

the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few.[3] Law enforcement officials have been frustrated by the inability of legislators to keep cyber-crime legislation ahead of the fast-moving technological curve.[4] At the same time, legislators face the need to balance the competing interests between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks.[5]

Further complicating cyber-crime enforcement is the area of legal jurisdiction.[6] Like pollution control legislation, one country can not by itself effectively enact laws that comprehensively address the problem of Internet crimes without cooperation from other nations. While the major international organizations, like the Organisation for Economic Co-operation and Development (OECD) and the G-8, are seriously discussing cooperative schemes, many countries do not share the urgency to combat cyber-crime for many reasons, including different values concerning piracy and espionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cyber-criminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another.

In section II of this article, we begin by providing an overview of cyber-crimes, the state of the law, and cyber-crime perpetrators and their motivations. Then, in section III we discuss in detail three major computer crimes and analyze how the different statutory subsections are applied depending upon the technical details of the crime itself. Just as a murder prosecution is dependent on *how* the crime was committed, different hacking techniques trigger different federal anti-

---

> agencies) detected computer security breaches within the last twelve months ... [s]eventy-four percent acknowledged financial losses due to computer breaches ... [and] [f]orty-two percent were willing and/or able to quantify their financial losses. The losses from these 273 respondents totaled $265,589,940 (the average annual total over the last three years was $120,240,180).

Id.

3. *See Federal Law Enforcement Response to Internet Hacking: Hearing of the Commerce, Justice, State and Judiciary Subcomm. of the Senate Appropriations Comm.*, 106th Cong. (2000) [hereinafter *Federal Response to Hacking*] (statement of Louis Freeh, Director, Federal Bureau of Investigation).

4. *See id.*

5. There is concern that the effort to fill the legal vacuum will include some protected rights, as was demonstrated by the Supreme Court's holding in *Reno v. ACLU*, 521 U.S. 844 (1997).

6. *See* Lee et al., *supra* note 2, at 873.

computer crime subsections. We begin with a discussion of the various denial of service attacks and the applicable statutes. Next we discuss the technical details of several hacking techniques and apply the relevant statutory subsections to the specific techniques. Finally, we explore the various types of computer viruses and how viral "payloads" and the class of the targeted computer will determine which federal subsection can be applied to the crime. In section IV, we discuss proposed legislative changes to the Computer Fraud and Abuse Act and related privacy concerns. Finally, we conclude this paper with a brief statement on the importance of tying together the technical elements of a cyber-crime and the application of the appropriate criminal subsection.

II. BACKGROUND

What is a cyber-crime? Law enforcement experts and legal commentators are divided. Some experts believe that computer crime is nothing more than ordinary crime committed by high-tech computers and that current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy. Others view cyber-crime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not deal with; such as jurisdiction, international cooperation,[7] intent, and the difficulty of identifying the perpetrator. Another source of confusion is the meaning of "hacker" and "cracker" and the distinction behind their motivations. The following section will elaborate on the differences between the two and their relevance to federal criminal statutes.

A. The State of the Law

Congress has approached computer crime both as traditional crime committed by new methods and as crime unique in character requiring new legal framework. For example, Congress has amended the Securities Act of 1933[8] to include crimes committed by a computer. However, Congress has also enacted a comprehensive new computer fraud and abuse section that can easily be amended to reflect changes in technology and computer use by criminals. In fact, the U.S. Congress has enacted statutes that widen the scope of

7. Michael A. Sussmann, *The Critical Challenges From the International High-Tech and Computer-Related Crime at the Millennium*, 9 DUKE J. COMP. & INT'L L. 451, 453-55 (1999).

8. 15 U.S.C. § 77(a)-(aa) (1994).

traditional crimes to specifically include crimes involving computers, or categorize them as entirely separate offenses. For example, the main federal statutory framework for many computer crimes is the Computer Fraud and Abuse Act (CFAA).[9] The statute is structured with an eye to the future so that it can be easily amended to reflect changes in technology and criminal techniques. The statute has already been amended several times to close unintended loopholes created by judicial interpretation. In its current form, the statute is very broad in scope, reflecting the government's resolve to combat cyber-crime at every level.

B. The Perpetrators—Hackers and Crackers

1. Hackers

"Hacker"[10] is a term commonly applied to a "computer user who intends to gain unauthorized access to a computer system."[11] Hackers are skilled computer users who penetrate computer systems to gain knowledge about computer systems and how they work.[12] The traditional hacker does not have authorized access to the system.[13] Hacking purists do not condone damage to the systems that are hacked.[14] According to The Jargon Dictionary, the term "hacker" seems to have been first adopted as a badge in the 1960s by the

---

9. 18 U.S.C.A. § 1030 (West Supp. 1999).

10. The term "hacker" has been defined as "[a] computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance." WEBSTER'S NEW WORD DICTIONARY OF COMPUTER TERMS 235 (7th ed. 1999). See Appendix A for a more detailed definition.

11. Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 310 n.7 (1993).

12. According to Deb Price and Steve Schmadeke, the "Hackers credo" is:

1. Access to computers should be unlimited and total.
2. All information should be free.
3. Mistrust authority—promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

Deb Price & Steve Schmadeke, *Hackers Expose Web Weakness: There's No Defense Against Internet Assaults, Experts Confess, and Attackers are Elusive*, DET. NEWS, Feb. 14, 2000, at A1, *available in* 2000 WL 3467302.

13. However, this is not a legal distinction. The Computer Fraud and Abuse Act criminalizes unauthorized access and access that exceeds authorization. *See* 18 U.S.C.A. § 1030(a)(1) (West Supp. 1999).

14. *See* Dissident, *Ethics of Hacking* (visited Mar. 3, 2000) <http://cultdeadbunnies.virtualave.net/hacking/lit/files/ethics.txt>.

hacker culture surrounding The Tech Model Railroad Club (TMRC) at Massachusetts Institute of Technology when members of the group began to work with computers.[15] The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.[16]

In the hacking "community," it is considered better to be described as a "hacker" by others than to describe oneself as a "hacker."[17] Hackers consider themselves members of an elite meritocracy based on ability and trade hacker techniques and "war stories" amongst themselves in Usenet forums, local or regional clubs, and national conferences, such as the annual Def Con Computer Underground Convention held in Las Vegas.[18]

2. Crackers

A "cracker" is a hacker with criminal intent.[19] According to The Jargon Dictionary,[20] the term began to appear in 1985 as a way to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. Crackers[21] maliciously sabotage computers, steal information located on secure computers, and cause disruption to the networks for personal or political motives.[22]

Estimates made in the mid-1990's by Bruce Sterling, author of *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, put "the total number of hackers at about 100,000, of which

---

15. *See* The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/h.html#hacker>.

16. *See generally* STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 10 (1984).

17. *See* Appendix A.

18. DEF CON is an annual computer underground party and conference for hackers held every summer in Las Vegas, Nevada. *See* DEF CON (visited Apr. 5, 2000) <http://www.defcon.org>.

19. The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/c/cracker.html>.

20. *See* Appendix A.

21. Please note that a "cracker" is different from a "crack." A crack is a script that defeats software protection codes, as opposed to using a circulated password that allows installation of the software. As software protection techniques become more sophisticated, the use of "cracks" have gained in popularity, as well as the challenge amongst crackers to defeat the protections. Most popular software passwords and/or cracks are widely available on the Internet. For example, one can quickly find software cracks by running a search on Astalavista (visited Mar. 9, 2000) <http://astalavista3.box.sk/>.

22. This distinction does not mean that hackers do not cause damage, but often it is their lack of intent that sets them apart from crackers, even though federal law does not always make such a distinction. *See* discussion *infra* on 18 U.S.C.A. § 1030 (West Supp. 1999).

10,000 are dedicated and obsessed computer enthusiasts. A group of 250-1,000 are in the so-called hacker 'elite', skilled enough to penetrate corporate systems and to unnerve corporate security."[23]

In the eyes of the law, hacking and cracking are not always treated the same way. Depending upon the method of intrusion, the type of computer that was broken into, the hacker's intent, and the type and amount of damage, different statutes and penalties will apply.[24] There are many ways to approach a discussion on hacking. In this article, we will structure the discussion on hacking techniques within the framework of the statutory elements to provide an understanding of how the different techniques trigger different statutes and penalties. We begin with an overview of hacking and an explanation of several common hacking techniques. Then, we discuss the relevant criminal code that can be applied depending on the nature of the hack.

C. Why People Hack

1. Hactivism

In recent years, according to the Department of Justice's National Infrastructure Protection Center, there has been a rise in what has been dubbed "hacktivism." Hacktivists launch politically motivated attacks on public web pages or e-mail servers. The hacking groups and individuals, or Hacktivists, overload e-mail servers by sending massive amounts of e-mail to one address and hack into web sites to send a political message.[25] In 1999, for example, the homepages for the White House, the U.S. Department of the Interior, White Pride, the United States Senate, Greenpeace, and the Ku Klux Klan were attacked by political activists protesting the sites' politics.[26]

---

23. *Cyberterrorism Hype*, JANE'S INTELLIGENCE REV., Dec. 1, 1999, at 48, 49, *available in* 1999 WL 8946130.

> However, to launch a sophisticated attack against a hardened target requires three to four years of practice in C, C++, Perl and Java (computer languages), general UNIX and NT systems administration (types of computer platform), LAN/WAN theory, remote access and common security protocols (network skills) and a lot of free time. On top of these technical nuts and bolts, there are certain skills that must be acquired within the cracker community.

Id.

24. *See* 18 U.S.C.A. § 1030(c) (West Supp. 1999).

25. *See Senate Joint Cyberattack Investigation: Capitol Hill Hearing Testimony*, 106th Cong. (2000) [hereinafter *Cyberattack Investigation*] (statement of Michael Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation).

26. *See Flashback Sweden* (visited Mar. 12, 2000) <http://www.flashback.se/hack/1999/>.

One such group is called the "Electronic Disturbance Theater," which promotes civil disobedience on-line to raise awareness for its political agenda regarding the Zapatista movement in Mexico and other issues.[27] Also, during the 1999 NATO conflict in Yugoslavia, hackers attacked web sites in NATO countries, including the United States, using virus-infected e-mail and other hacking techniques.[28] On February 7, 2000, the official web site of the Austrian Freedom Party was hacked to protest the inclusion of Jörg Haider and his party into a coalition Austrian government.[29]

2. Employees

According to a study conducted in 1999 by Michael G. Kessler & Associates Ltd., disgruntled employees are the greatest threat to a computer's security.[30] Employees that steal confidential information and trade secrets account for thirty-five percent of the theft of proprietary information.[31] In fact, data suggests that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimized organization rather than to outside hackers with modems.[32] Internet Security Systems' Chris Klaus estimates that over eighty percent of the attacks on computer systems are committed by employees.[33]

According to recent FBI assessments, disgruntled insiders are a principal source of computer crimes.[34] Insiders do not need a great deal of knowledge about their target computers, because their inside knowledge of the victim's system allows them unrestricted access to

---

27. *See Federal Response to Hacking, supra* note 3.

28. *See id.*

29. To view a copy of the hacked web site, see (visited Apr. 9, 2000) <http://www.flashback.se/hack/2000/02/07/1/>.

30. *See* David Noack, *Employees, Not Hackers, Greatest Computer Threat* (Jan. 4, 2000) <http://www.apbnews.com/newscenter/internetcrime/2000/01/04/comptheft0104_01.html>.

31. *See id.*

32. *See* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalizaton: The Case of Computer Crime Laws,* 26 CRIMINOLOGY 101, 116 (1988).

33. Matthew Nelson, *Internet Security Systems' Chris Klaus says companies should close back doors to be secure,* INFOWORLD, Jan. 10, 2000, at 40a. According to a recent survey of 643 computer security practitioners in the U.S., 71% reported unauthorized access by insiders. *See* CSI Survey, *supra* note 2.

34. *See* Congressional Statement, Federal Bureau of Investigation, *National Infrastructure Protection Center (NIPC) Cyber Threat Assessment, October 1999, Before the Subcomm. on Technology and Terrorism of the Senate Comm. on the Judiciary* (Oct. 6, 1999) <http://www.y2kcoming.com/cyber/nipc10_99.htm> (statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation).

cause damage to the system or to steal system data.[35] A Computer Security Institute/FBI report notes that fifty-five percent of survey respondents reported malicious activity by insiders.[36] Employees who exceed their authorized use and intentionally cause damage are just as liable as an outside hacker who intentionally causes damage.[37] However, § 1030(a)(5) of the CFAA does not criminalize damage caused by authorized persons and company insiders that was reckless or negligent.[38] Only outside non-authorized hackers are liable for *any* damage caused, whether it was negligent, reckless, or intentional.[39]

3. Recreational Hackers

"Recreational hackers" break into computer networks for the thrill of the challenge or for bragging rights in the hacking community.[40] While hacking once required a fair amount of skill or computer knowledge, the recreational hacker today can now download attack scripts and protocols from the Internet and launch them against victim sites with little knowledge of the systems they are attacking.[41] There are countless web sites on the Internet that provide "newbies" (inexperienced hackers, or "wannabes") with detailed instructions on hacking techniques and downloadable, do-it-yourself hacking tools.[42] In recent years, the hacker's attack tools have become more sophisticated and easier to use.[43] For example, in 1999 hackers defaced the Anniston Army Depot, Lloyd's of London, the U.S. Senate and Yahoo home pages to demonstrate to the hacking community their ability to hack into third-party servers and to highlight the servers' vulnerabilities.[44]

---

35. *See id.*

36. *See id.*

37. 18 U.S.C.A. § 1030 (West Supp. 1999).

38. *Id.* § 1030(a)(5).

39. *See id.* § 1030(a)(5)(C).

40. *See Cyberattack Investigation, supra* note 25.

41. *See* Internet Security Systems, *Back Orifice 2000 Backdoor Program* (visited Apr. 5, 2000) <http://www.iss.net/customer_care/resource_center/whitepapers> [hereinafter *Back Orifice*].

42. Hackers learn hacking techniques from a variety of sources, including high school and university computer groups; newsgroups such as alt.2600.hackerz and alt.binaries.hacking.beginners; hacking web sites such as <http://www.flashback.se> and <http://www.lopht.com/>; as well as hacking search engines, such as <http://astalavista.box.sk/>.

43. *See Cyber Threat Assessment, supra* note 34.

44. *See Flashback Sweden, supra* note 26.

4. Web Site Administrators and Web Pages

It is usually considered a passive and harmless exercise to visit a web site. The user requests information and the server responds to the request by sending out packets of requested data back to the user's computer. However, web sites can also access a lot of hidden background information from the user. For example, Privacy.net has a web site that will show users all of the information that can be taken from their individual computer.[45] The remote web site can determine the following information about a visitor:

(a) the IP address the user is accessing the web site from;

(b) the number of prior visits to the web site, and the dates;

(c) the URL of the page that contained the link to get the user to the web site;

(d) the user's browser type and operating system and version;

(e) the user's screen resolution;

(f) whether JavaScript and VBScript are enabled on the user's computer;

(g) how many web pages the user has visited in the current session;

(h) the local time and date; and

(i) FTP username and password, if there is one.[46]

Privacy advocates have pressured web browser developers to address security concerns by enabling users to significantly enhance their privacy by adjusting the security level on their browsers. The extent of information that a web site can retrieve from a visitor without violating the CFAA is still uncertain. Section 1030(a)(2)(C) proscribes the intentional access of computer information. When a person visits a web site, how much information has that person reasonably "authorized" the web site to obtain? This question may be answered by a court in one of the cases filed against RealNetworks over its gathering of user data.[47]

---

45. *Privacy.net: The Consumer Information Organization* (visited Mar. 5, 2000) <http://privacy.net/analyze/>.

46. *Id.*

47. In November, 1999, it was alleged that "RealNetworks' popular RealJukebox software... surreptitiously monitors the listening habits and certain other activities of people who use it and continually reports this information, along with the user's identity, to RealNetworks." Sara Robinson, *CD Software Is Said to Monitor Users' Listening Habits*, N.Y.

It is also possible for a web programmer to enable a web page to send an e-mail to a predetermined address just by visiting the page through a JavaScript exploit in Netscape Navigator Versions 2.0 through 4.0b1.[48] For example, if a person visits such a web site, hidden within the hypertext markup language (HTML) is code that will cause the person's e-mail program to send an e-mail to the web site with the person's e-mail address in the "from" slot. Theoretically, this exploit would allow a web site to collect all of the e-mails from persons who visit their web site. Internet Explorer and Netscape Navigator provide security warnings to users before they send the mail if the security level is set at a higher level.[49]

III. TYPES OF COMPUTER CRIME

In this section, we begin by providing an overview of cyber-crime and criminal techniques used to penetrate protected computer networks, including: (1) Denial of Service attacks; (2) web site defacing and malicious interference; and (3) malicious code—viruses, worms, and Trojans. We then discuss in detail the CFAA, how it is applied, and how it has changed over the past decade. We also look at other laws that the federal government uses to control computer crimes.

A computer can be the target of the offense, the tool used in the offense, or may contain evidence of the offense.[50] An understanding of the different uses of a computer will provide the foundation of the application of the criminal statutes.

The computer is an indispensable tool for almost all cyber-

TIMES, Nov. 1, 1999 at C1. A security expert discovered that RealNetworks was using its RealJukebox player to secretly scan the hard drives of computers and send the information about the user's musical content and preferences to the company. The software also created a serial number to identify the user. *See id.* As a result, three class-action lawsuits were filed against RealNetworks. Two federal lawsuits, filed in Pennsylvania and Illinois, alleged that the company violated the Computer Fraud and Abuse Act by secretly collecting personal information without the user's consent. The lawsuits claim that this is a violation of federal law because RealNetworks accesses information on a protected computer without the knowledge of the user. *See* Greg Miller, *RealNetworks Breached Privacy, 3 Suits Contend Consumers: Firm Admitted Collecting Data on Users of its Internet Software, Provoking the First Class Actions in Such a Case*, L.A. TIMES, Nov. 11, 1999, at C1.

48. *See DigiCrime E-mail Address Demonstration* (visited Mar. 5, 2000) <http://www.digicrime.com/noprivacy.html>; *see also Onion Routing* (visited Mar. 5, 2000) <http://www.onion-router.net/Tests.html> (listing other good privacy testing sites).

49. For example, Microsoft Internet Explorer provides four levels of security on its web browser, ranging from low to high. The various levels of security allow the user to make a tradeoff between unimpeded access to all Internet content and security concerns.

50. *See* Hatcher et al., *supra* note 1, at 401.

crimes. However, as more devices are enabled to communicate with the Internet, the hackers arsenal of tools is likely to multiply.[51]

When a computer is the target of the offense, the criminal's goal is to steal information from, or cause damage to, a computer, computer system, or computer network.[52] Hacking, cracking, espionage, cyber-warfare, and malicious computer code viruses are common forms of crimes that target the computer. The perpetrators range from teenage "cyber-joyriders" to organized crime operations and international terrorists. According to a survey conducted by Michael G. Kessler & Associates Ltd., a New York security firm, computer theft of proprietary information is committed by discontented employees (35%), outside hackers (28%), other U.S. companies (18%), foreign corporations (11%), foreign governments (8%), and miscellaneous (10%).[53]

The computer may also be a tool of the offense. The criminal uses the computer to commit a traditional crime, such as counterfeiting. For example, a counterfeiter that used to engrave plates to create the counterfeit currency can now use sophisticated graphic computers with advanced color printers. An example of a computer used to perpetrate a traditional crime is the extortion attempt by George Matos Rocha from North Carolina.[54] Mr. Rocha was charged with bombing three home improvement stores and subsequently threatened the retail chain to continue the bombings unless he received $250,000.[55] Using the Internet, Mr. Rocha set up a bank account in Latvia and instructed the company to wire the extortion money to his Latvian account.[56] The FBI was able to identify the account and trace its origin back to the United States with the help of his Internet Service Provider. Mr. Rocha pleaded guilty in

51. LOpht Heavy Industries is developing a hacking platform based on the PalmPilot, mainly because of its high-mobility and the ability to communicate with desktop computers. LOpht already offers several applications for PalmPilots that demonstrate its potential as the next hacker's development platform. The ability to communicate using wireless infrared communication, the small size and the support for TCP/IP makes PalmPilot almost ideal for physical penetration to a local network. *See LØPHT Heavy Industries* (visited Mar. 19, 2000) <http://www.lopht.com>; *see also* Phil Askey, *How to Connect Your PalmPilot to Windows NT*, Jagtech (1997) <http://www.jagtech.com.au/Docs/pilot_nt.htm> (copy on file with the author).

52. *See id.*

53. *See* Noack, *supra* note 30.

54. *See* Paula Christian, *Lowe's Bombing Suspect Pleads Guilty; A Greensboro Man Will Face at Least 37 Years in Prison When He is Sentenced in March*, GREENSBORO NEWS AND REC., Dec. 7, 1999, at A1, *available in* 1999 WL 26311607.

55. *See id.*

56. *See id.*

December to explosives charges and extortion. He could have faced life in prison.[57]

Computers can also be incidental to the offense, but are nevertheless important because they contain the evidence of a crime. Money launderers, for example, may use a computer to store details of their laundering operation instead of relying on paper accounting records. Child pornographers' computers are often seized as the key evidence[58] that the defendant produced, possessed, received, and/or distributed child pornography.[59]

A. Denial of Service

A Denial of Service (DoS) attack is a rather primitive technique that overwhelms the resources of the target computer which results in the denial of server access to other computers. There are several different techniques that hackers use to "bring down" a server. As the network administrators learn how to limit the damage of one technique, hackers often create more powerful and more sophisticated techniques that force system administrators to continually react against assaults. In order to understand how to apply the law to these attacks, a basic understanding of the anatomy of the attacks is

57. *See 40 Years Meted in Lowe Bombings, in* Henry Bailey, U.S. & WORLD NEWS IN BRIEF, COM. APPEAL (Memphis TN), Mar. 10, 2000, at A5, *available in* 2000 WL 4444494.

58. *See, e.g.*, United States v. Snyder, 189 F.3d 640 (7th Cir. 1999). James Snyder was convicted of producing, receiving, and distributing child pornography, as well as possessing child pornography with intent to sell. Mr. Snyder engaged in a sexual affair with a minor child. After the minor was interviewed by the FBI and was able to describe the abuse and identify Mr. Snyder's house, a search warrant was obtained and served on Mr. Snyder. The computer-related evidence seized from Snyder's house was "analyzed by the FBI crime lab . . . [and] verified that Snyder's computer was capable of downloading and uploading images from the Internet, and that it could be hooked up to a camera. [The FBI] also recovered several pornographic images from the computer, even though they had been deleted." *Id.* at 644.

59. *See, e.g.*, United States v. Simons, 29 F. Supp. 2d 324 (E.D. Va. 1998). Mark Simons was an employee of the Foreign Bureau of Information Services (FBIS) component of the CIA. While a FBIS network administrator was doing a routine check of the agency's firewall, he noticed a lot of activity from one work station going to a pornographic site, against established agency rules. The computer was seized as evidence and Mr. Simons was charged with violating 18 U.S.C. § 2252A(a)(2)(A) (1994), Receiving Materials Containing Child Pornography, and 18 U.S.C. § 2252A(a)(5)(B), Possession of Material Containing Child Pornography. Mr. Simons unsuccessfully challenged the seizure on grounds that the search was a violation of the Fourth Amendment. The court held that, in applying the holding in *Katz v. United States*, 389 U.S. 347 (1967), the court must consider "whether the employee searched had a reasonable expectation of privacy. The person must have had an actual or subjective expectation of privacy and the expectation must have been one that society recognizes as reasonable." United States v. Simons, 29 F. Supp. 2d at 326-27. The FBIS has a specific policy providing for computer audits and given this policy, the court concluded that Mr. Simons did not have a "reasonable expectation of privacy with regard to any Internet use." *Id.* at 327.

necessary.[60]

There are basically three main network exploits that are used to overwhelm a system's server: SYN Flood Attacks, UDP Flood Attacks and ICMP Flood Attacks. Each technique exploits a weakness in the way computers communicate amongst each other over the Internet. A basic understanding of the TCP/IP Internet protocols is helpful to differentiate between the techniques.

Internet Protocols:

The Internet is a network of computers that are connected so they can exchange information amongst each other. The computer that is asking for information from another computer is the "client" and the computer that is receiving the request is the "server." When the client wants to receive information that is located on the server, it sends a request for the information. However, the computers must establish a connection before data can be exchanged. The server needs to know who it is going to send the information to and needs to make sure the client computer is ready to receive the information. This is considered a "3-way handshake." The first part of the handshake occurs when the client computer sends a message to the server with a "SYN flag" that tells the server how to identify it.[61] Second, upon receiving the request, the server will send out its own identification number, called an Initial Sequence Number (ISN) in a SYN for this request and an acknowledgement (ACK) of the client's request. In the third part of this "handshake," the client computer receives the SYN and ACK from the server and sends back the ACK with the server's numbers, like a secret code the two of them share so the server can keep track of multiple clients. Now the data transfer can take place. In summary, the client sends a message to the server, the server sends back a message to the client that the server is "awake" and ready to process the requests, then the client sends back an acknowledgement that it is ready to receive. This may seem redundant, but the need to establish the connection on both sides is

60. Many commentators equate a DoS to a store front being blocked by hundreds of protestors to deny legitimate customers from entering the store. A more accurate analogy would be sending a hundred people into a store who overwhelm the sales staff, rendering them unable to respond to legitimate customers. Eventually, the store becomes so crowded that a line forms outside, where the "bogus" customers and real customers queue up, denying access to legitimate customers.

61. A "SYN" packet is an abbreviation for "synchronized/start." The SYN packet is the packet that originates with the "source host," or the person initiating the communication. The SYN packet is part of the TCP "3-way handshake."

very important, because the data is broken up into small packets by the server and sent out over the Internet to the client. The client needs to know how to organize the data puzzle as the packets arrive and the client also needs to know if any packets are missing. As each piece of the puzzle arrives, the client lets the server know the piece has been received, so the server knows if it has to re-send it.

TCP/IP stands for Transmission Control Protocol and Internet Protocol.[62] Basically, the TCP is the workhorse of the communication on both sides. If a file is requested by the client, the server locates the file on its computer and breaks the file into tiny pieces. The tiny pieces are called datagrams. Each datagram is "wrapped" in a bundle of instructions that tells it where to go. These little bundles are called "packets." The TCP assigns a sequence number to every byte transferred so it can track what it has sent and eliminate the need to duplicate sending the same packet twice unless the packet is lost somewhere along the line to the client. The "packet header," contains the sequence numbers that also tells the client the next sequence number to expect after each packet, so the client can start arranging the packets and conduct a rolling inventory. The TCP acts as a digital shipping and receiving department.

The job of the Internet Protocol (IP) is easier. The IP's job is to route the packets across the Internet to the client. Each computer on the Internet has an IP address that tells the computers where the other is located. The IP address is very similar to a zip code. For example, a zip code that begins with a 9, belongs to an address located on the west coast of the United States. If the next number is a 4, the location is in the San Francisco area, and so on until the precise region is located. However, to parallel the IP addresses, each house in the zip code area would be assigned a number, instead of an address. So when a client or server sends a packet out over the Internet, the packet is "routed" through many other servers to reach its final destination. The IP tacks on the numerical address and ships it out, hoping the packet arrives where it is supposed to go. If the server does not receive a response that the packet was received on the other end, the IP can send an error message to the client, called an Internet Control Message Protocol, or ICMP, letting the client know that the packet did not get there. It is this system of trust and cooperation between the computers that is exploited by a denial of service attack.

62. *See* Appendix A.

1. SYN Flood Attacks

One of the weaknesses in the system is the amount of SYN requests the TCP can handle. When the TCP receives more requests than it is programmed to handle, it puts the other incoming SYN requests in a queue. When the queue is filled to capacity, there is no more room to put the other incoming SYN requests and they are turned back. Hence, they are "denied service."

Another technique is to slow down the TCP process by making the TCP wait for all of the ACKs it sent out to be acknowledged by the client. When the attacker sends a message to the server requesting data, the server sends out a SYN and an ACK and waits to hear back from the attacker's client, as part of the third part of the 3-way handshaking. However, the attacker has "spoofed" his return address so that the server sends a "self-addressed and stamped" envelope to an address that is either false or belongs to a computer that is not responding. If enough of these "spoofed" SYN messages are sent, the server is paralyzed by its wait for non-existent confirmations. "SYNK" is a common SYN flood program that is widely downloadable on the Internet.[63]

2. UDP Flood Attacks

User Datagram Protocol (UDP) flood attacks work in very much the same manner as the SYN Flood attacks. In a server, the UDP provides information about the server to other computers, such as the server's local time, echo, chargen, etc.[64] When the server is hit with multiple requests for information about itself, the server can be quickly overwhelmed by its inability to process so many UDP packets. The result is total consumption of the server's processing power and bandwidth, thereby "denying service" to others who are trying to access the server. The problem is multiplied when a hacker connects one computer's chargen port with another's echo port. The result is the generation of a massive amount of packets that overwhelm the system and render it useless.[65]

63. SYNK, along with other DoS tools, is available on many hacking web sites. For example, SYNK can be obtained at Warmaster's web site. *See Warmaster* (visited Apr. 5, 2000) <http://www.warmaster.de/linw.htm>.

64. For example, the UDP "echo" provides a port that returns every packet sent to it. The UDP "chargen" returns a packet with 0 to 512 characters chosen randomly. The UDP "time" protocol provides the time in a site-independent, machine readable format. The client sends an empty datagram to the port, and the server sends a datagram containing the time as a 32 bit binary number.

65. *See CERT Coordination Center Report CA-96.01: UDP Port Denial-of-Service Attack*

3. ICMP Flood Attack

The Internet Control Message Protocol (ICMP) flood attack is also similar to the above flood attacks. The ICMP is used to handle errors and "pings." Pings are small "feelers" that are sent out to other computers to see if they are turned on and connected to the same network.[66] Ping is also used to determine if there is network congestion and other network transport problems. When a ping packet is sent to an IP broadcast address from a computer outside of the remote computer's network, it is broadcast to all machines on the target network.

The ICMP attack begins when a large number of forged ping requests are sent to a broadcast address on a third-party's server. These packets contain the return address of the intended victim. The flood of ping requests causes the targeted server to answer with a flood of responses which can cause both the target site and third-party sites to crash.[67]

A variation on the ICMP attack is the "Ping of Death." The Ping of Death is a large ICMP packet that is sent to the target server. The target receives the ping in fragments and starts to re-assemble the packets as they arrive. However, the completed size of the packet is larger than the buffer, or than the room the computer has allocated to such packets, and the computer is overwhelmed, often resulting in the server shutting down or freezing up.[68]

4. New Generation Attacks

a. Smurf Attacks

These techniques are named after the programs that launch the

(visited Mar. 17, 2000) <http://www.securityfocus.com/templates/archive.pike?list=21&date=1996-02-08&msg=v02120d01ad4092622ff2@[128.115.138.237]>.

66. *See GUIDE TO (mostly) HARMLESS HACKING* (visited Mar. 12, 2000) <http://newdata.box.sk/neworder/harmless/GTMHH2-3.TXT>.

67. As an example of this type of attack, consider the following: To launch a ping attack, the attacker, using Computer A, gets the IP address of a computer he wants to bring down. If Computer A is using Windows, all the attacker needs to do is go to the DOS prompt and enter "c:\windows\ping -1 65510 targeted.computer.com." This command creates a giant datagram that gets wrapped inside a packet that is sent to targeted.computer.com and overloads the targeted computer as it tries to send the pin back. It is a very simple technique, and just as easy to get caught if the attacker used his computer to launch the ping attack. However, the attacker will typically spoof his location, making discovery more difficult.

68. *See The Hack FAQ - Denial of Service Basics* (visited Mar. 12, 2000) <http://www.nmrc.org/faqs/hackfaq>.

attacks. In a Smurf attack, the hacker sends out an ICMP echo request packet, or "ping" command to a computer network with the return IP address of the targeted victim. The network's server broadcasts the "ping" through the system's network and the computers send a reply back. If the network is large enough, those packets will swamp the victim's computer and possibly bring the computer down.[69]

b. Fraggle

The Fraggle attacks are similar to the Smurf attacks, except they use UDP echo packets to overwhelm a network computer.

c. Papasmurf

Papasmurf combines Smurf and Fraggle by launching ping requests with ICMP echo packets and UDP echo packets. This program's two-headed assault makes it more difficult for administrators to defend themselves.

5. Distributed Denial of Service Attacks

Distributed Denial of Service attacks (DDoS) are a natural development in the search for more effective and debilitating denial of service attacks. Instead of using just one computer to launch an attack, the hacker enlists numerous computers to attack the target computer from numerous launch points.[70] Prior to an attack, the hacker places a daemon, or a small computer program, on an innocent third-party computer. These third-party computers are often referred to as "zombies" or "soldiers." The "slave" daemons are remotely controlled by the "master" program to launch attacks against certain servers. By distributing the source of attacks across a wider array of zombie computers, the attacker has made it more difficult for the target server to block off the attack routes.

a. Trinoo (June 1999)

On August 17, 1999, a Trinoo network of at least 227 systems was used to flood a single server at the University of Minnesota, including more than 100 compromised computers at the University of

69. *See* Carnegie Mellon Software Engineering Inst., *CERT® Advisory CA-98.01 "smurf" IP Denial-of-Service Attacks*, (originally issued Jan. 5, 1998) (last modified Mar. 13, 2000) <http://www.cert.org/advisories/CA-98.01.smurf.html>.

70. *See* Brian Martin, *Have Script, Will Destroy (Lessons in Dos)*, HACKER NEWS (visited Mar. 13, 2000) <http://www.hackernews.com.bufferoverflow/00/dosattack/dosattack.html>.

Washington.[71] The attack rendered the system inoperable for two days.

There has been speculation that Trinoo was one of the programs that brought down Yahoo and other major Internet sites in February 2000.[72] Trinoo is used to create distributed denial of service UDP flood attacks. There is concern that Trinoo could enlist common desktop computers in a DDoS attack by loading a daemon on the local computer through an e-mail attachment.[73] According to one estimate, Trinoo networks are "being set up on hundreds, perhaps thousands, of systems that are being compromised by remote buffer overrun exploitation."[74]

After the attacker has placed the daemons on the intermediary computers, master programs are set up on other computers to act as commanders to call "the troops" into action. The attacker only needs to access the master programs, via telnet, to launch the massive, coordinated attacks.[75] Both the slave and master programs are password controlled to prevent system administrators from taking control of the Trinoo network. Once the attacker has accessed the master, he only needs to enter the IP address of the targeted server in a "dos IP" command to wake up the daemon "zombies" that begin launching their massive queries at the target. The attacker is also able to launch attacks against multiple targets using the "mdos" command.[76] Finally, the attacker can set a time limit for the DoS attack.[77]

b. Tribe Flood Network (August 1999)

Tribe Flood Network, (TFN), is a DDoS program written by a

---

71. *See* Bruce V. Bigelow, *Net's Newest Pains Most Likely Caused by Feuding Hackers,* SAN DIEGO UNION-TRIB., Feb. 10, 2000, *available in* 1999 WL 29194212.

72. *See* John Borland, *New Attack Software Released; Web Sites Now Easier Targets For Hackers,* SEATTLE-POST INTELLIGENCER, Feb. 24, 2000, at E2, *available in* 2000 WL 5289421.

73. *See* John Borland, *Hackers Spread Simpler Tools for Vandals,* CANBERRA TIMES, Feb. 28, 2000, at A13.

74. David Dittrich, *The DoS Project's "Trinoo" Distributed Denial of Service Attack Tool,* (Oct. 29, 1999) <http://www.ussrback.com/docs/distributed/trinoo.analysis.txt> [hereinafter Dittrich, *DoS Project*]. "A buffer overrun is when a program allocates a block of memory of a certain length and then tries to stuff too much data into the buffer, with the extra overflowing and overwriting possibly critical information crucial to the normal execution of the program." *Exploiting Windows NT 4 Buffer Overruns A Case Study, RASMAN.EXE* (visited Mar. 17, 2000) <http://newdata.box.sk/neworder/ntbufferoverruns.txt>.

75. *See* Dittrich, *DoS Project, supra* note 74.

76. *See id.*

77. *See id.*

German hacker that is capable of launching ICMP, SYN Flood, UDP Flood and Smurf attacks.[78] In late August, 1999, DDoS attackers began to shift from Trinoo to TFN. Using TFN, a single attacker can launch an attack from dozens of computers on which the attacker has surreptitiously placed the TFN daemon.[79] The attacker remotely controls the TFN client network using a variety of connection methods, including telnet TCP connections.[80] Unlike various versions of Trinoo, TFN clients do not require a password to be activated, although the client sends commands to the daemon in an ICMP packet. However, there is no telnet TCP or UDP-based communication between the client and the daemon, making detection of the client's call to action more difficult to detect on the client, or master, system.[81]

c. *Tribe Floodnet 2k (January 2000)*

Tribe Floodnet 2k (TFN2K) is an updated version of the TFN DDoS attack tool. According to Mixter, the German hacker who wrote the program, TFN2K still contains the popular features of the original TFN, including the client/server functionality, stealth, and encryption techniques. However, Mixter added several new features that make the system more robust and deadly, including remote one-way command instructions to the distributed servers who go on to launch the attacks. Also, TFN2K boasts stronger encryption between the client and the server.[82]

---

78. *See* David Dittrich, *The "Tribe Flood Network" Distributed Denial of Service Attack Tool*, (Oct. 21, 1999) <http://www.ussrback.com/docs/distributed/tfn.analysis.txt > [hereinafter Dittrich, *Tribe Flood Network*].

79. *See Anatomy of an Attack*, THE ECONOMIST, Feb. 19, 2000, at 80, 81.

80. *See* Dittrich, *Tribe Flood Network, supra* note 78. Once the hacker has placed the software on several client computers, the hacker needs to give commands to the client machines to call them into battle. This is done through a variety of connection methods, including common telnet connections. The client machines control the daemons who launch the attacks against the final targets. The hacker can be thought of as a general in the Pentagon and the clients are the field commanders orchestrating the combat units in an assault.

81. According to the *readme.txt* that is downloaded with the TFN program, the system is easy to operate: "Usage: Install the server 'td' on a number of hosts. Put all IP addresses of the hosts running the server into a list; this will be your iplist. Run the client." *Id.*

82. As an example of this type of attack, consider the following: If the attacker, using computer A, wanted to launch a DDoS assault on Computer F, then he would install "servers" on Computers B, C and D. Computer A can give instructions to B, C and D by randomly choosing to send the command on TCP, UDP or ICMP protocols. The internal values, or the packet's "identification papers," are optimized by the software so there is no identifiable pattern to the packets that would otherwise cause a server or router's filtering method to reject it. Then the TFN servers that were placed on Computers B, C and D decode the message that contains Computer A's spoofed, or false identification papers and begin launching an attack against

d. Stacheldraht (October 1999)

The most recent advance in DDoS attacks has come in the form of Stacheldraht, a German word for "Barbed Wire." Stacheldraht has the ability to automatically update the daemon programs, reducing the attacker's risk of intrusion.[83] Stacheldraht was based on the source code from Tribe Flood Network, with at least two significant new features. The communication between the attacker and the Stacheldraht masters are encrypted and the daemons can be automatically updated by the masters. One of the weaknesses of TFN was the attacker's connection to the master program located on the remote computers.

Stacheldraht combines Trinoo's master/daemon control features with TFN's ICMP flood, SYN flood, UDP flood, and Smurf attacks.[84] The attackers control the master computers through encrypted clients, and each master can control up to 1000 daemons that are installed on innocent third-party computers.[85] The attack begins in the preparation stage, called the "mass-intrusion phase," where large numbers of computers are compromised.[86] The attacker places the Stacheldraht daemons on the compromised systems and the daemons lie in wait for the command to attack. The third-party computers are also victims in these attacks because the systems have been compromised and they use up bandwidth and processing power.

6. Tracking Down the Attackers

The Federal Bureau of Investigation (FBI) has had a very difficult time locating the origin of the attackers because of the networked nature of the Internet, the spoofing of the DoS packets, and the procedural difficulty of organizing an investigation that involves countless jurisdictions. One method used to track the attacker is to start from the targeted server and locate the immediate server that sent the packet.[87] However, because the packet was carrying "false

---

Computer F. In order to further trip up egress filtering, custom IP addresses may be used to defeat the spoof filtering defense. Also, the program allows decoy packets to be sent out to Computers G to Z to hide the real location of Computers B, C and D that contain the TFN servers.

83. *See Anatomy of an Attack, supra* note 79 at 81.

84. *See* Dave Dittrich, *The "stacheldraht" distributed denial of service attack tool* (Dec. 31, 1999) <http://www.ussrback.com/docs/distributed/stacheldraht.analysis> [hereinafter Dittrich, *Stacheldraht*].

85. *See id.*

86. *See id.*

87. *See* Martin, *supra* note 70.

identification," each subsequent router along the network could lead the investigator astray.[88]

Because the packet's "false papers" hide the true origin of the packet, it is difficult to reconstruct the origin of the spoofed packets after the fact. In order to determine where the packet came from, the investigators must set up a filer, or "trace and trap," before they arrive at that particular router. This is complicated by fact that the packet could cross as many as thirty different routers owned by ten different companies in several different legal jurisdictions.[89] In the February, 2000 attacks on the major Internet sites, the authorities have identified several university computers that were compromised and used to attack the targeted servers.[90]

The actual technique of spoofing can be complicated. For example, a traditional method of spoofing was to initiate a DoS attack on Computer B, the computer that one eventually wants to spoof. When Computer B is overwhelmed, it is not able to respond to requests from Computer C that it is requesting ACKs, or confirmation—trying to confirm they are who they said they are. The TCP tags each datagram with a sequential number. If Computer C receives a packet that is out of sequence, it will discard the packet or hold, depending on how close the packet is to the number it is looking for. The hacker, using Computer A, estimates the number that Computer C is looking for and pretends to be sending packets from Computer B by using Computer B's information or identification. Computer B is unable to stop this use of his identification because he is spending all of his time answering the false packets from another

88. Mixter, the German hacker who authored Tribe Flood Network, comments that "[i]t will be virtually impossible to track the attackers down.... Every provider would have to scrutinize their router logs tracing back traffic to its point of origin, and that's a time-intensive process and an enormous undertaking." Iain S. Bruce, *The Hack Pack,* SUNDAY HERALD, Feb. 13, 2000, *available in* 2000 WL 4100421.

89. *See "Trap and Trace" Authority on the Internet Urged by DOJ, FBI,* COMM. DAILY, Mar. 2, 2000, *available in* 2000 WL 4694585 [hereinafter *Trap and Trace*].

90. According to the Department of Justice, the federal trap and trace statutes (18 U.S.C. §§ 3121-3127 (1994)) are out-of-date with Internet investigative requirements. "Pen registers" that record dialed telephone numbers and the trap and trace devices that capture incoming electronic packets to identify their origin, are not specifically covered by the statutes. Rather, the statute refers to a "device" that is "attached" to a telephone "line." *See* 18 U.S.C.A. § 3127(3) (1994). However, traffic on the Internet is not traced by telephone number, but rather by IP addresses and other information wrapped inside the packets. Also, telephone companies no longer physically connect devices to lines to route calls and Internet traffic. Instead, calls and traffic are routed by a series of electronic switches, often without wires. *See* Department of Justice, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet - A Report of the President's Working Group on Unlawful Conduct on the Internet* (Mar. 2000) <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>.

computer that the hacker has set up to send the packets.

7. The CFAA and Denial of Service

In any criminal law analysis, the specifics of the crime will determine which statutory section can be successfully applied. For example, the exact definition of an "intrusion" can determine whether inserting a debit card into a exterior cash machine constitutes burglary. The individual characteristics of a Denial of Service attack may also change which computer crime statutes can be applied to the attack. For example, in the above TFN2K example where the attacker used Computer A to plant "servers" on Computers B, C, and D to attack Computer F, will a traditional hacking statute be applicable for the attack on Computer F? Under 18 U.S.C. § 1030(a)(5)(B) and (C), the statute prohibits "access" of a protected computer.[91] However, are these anti-hacking statutes applicable to an attacker whose intent was to "deny access" to, rather than to merely access, the computer?

The CFAA is the primary federal anti-hacking statute, and contains seven main sections. The first section, § 1030(a)(1), protects against the knowing access of government computers to obtain classified information. This section is not applicable.

The second section, § 1030(a)(2), proscribes the intentional access of a computer without, or in excess of authorization, to thereby obtain information from a financial institution, the federal government, or any protected computer involved in interstate or foreign communications—essentially any computer connected to the Internet.[92] This section is concerned with the protection of information. The point of all of the DoS attacks is not to obtain information, but rather to bring the system down.

The third section, § 1030(a)(3), is concerned with the intentional and unauthorized access of government computers or computers used by the government. In a standard DoS attack where only one computer is used to attack another, this section is unlikely to be invoked unless the attacker targeted a computer that "is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States."[93] However, in a DDoS attack, there is a better chance that this section may be relevant if the attacker placed an attack daemon on a § 1030(a)(3) protected computer. Many university computers, for example, are used by the

91. *See* 18 U.S.C.A. § 1030(a)(5)(B)-(C) (West Supp. 1999).

92. *See* Hatcher et al., *supra* note 1, at 403.

93. 18 U.S.C.A. § 1030(a)(3).

federal government. Even slight activity by the daemon on the university computer could "affect" the government's use of the computer.

The fourth section, § 1030(a)(4), addresses the access and fraudulent use of a protected computer and is triggered if the value of the use obtained exceeds $5,000. Congress intended this subsection to apply, for example, to use by hackers who take over a supercomputer to run a password-breaking program. The "zombie" computers who were infected by the daemon and enlisted into the attack suffered a loss of processor power and bandwidth. This subsection could be applied against the attacker for each computer the hacker enlisted in the assault. With the subsection providing for a jail term for up to five years per instance, a hacker who plants hundreds of daemons could be liable for an extensive prison sentence.

One of the critiques of this subsection is the $5,000 damage threshold. Prosecutors have found that the $5,000 damage requirement is often both difficult to establish and an impediment to investigation. It is sometimes speculative to assess $5,000 damages if the attacker only used the computer to launch attacks. In *United States v. Middleton*,[94] the defendant challenged the government's theory of calculating the $5,000 in damages to Slip.net, an Internet Service Provider (ISP). The court held that the government's theory of loss "will be that the damage caused by defendant to the Slip.net computers caused Slip.net employees to expend time to investigate, identify, and correct the damage caused by Middleton, and take other security related steps."[95] The court agreed with the government "that the time the employees expended can be fairly valued at a figure of at least their hourly wage or salary, plus the value of benefits and overhead" provided adequate explanation of the government's theory.[96]

In addition to the uncertainty concerning the factors used to calculate the $5,000, federal authorities currently have to wait for a damage assessment to determine if there is federal jurisdiction,

---

94. 35 F. Supp. 2d 1189 (N.D. Cal. 1999).

95. *Id.* at 1193.

96. *Id*; *see also United States Sentencing Commission, Sentencing Guidelines for United States Courts, Part II*, 62 Fed. Reg. 26616 (1997), *available in* 1997 WL 243415, which states:

> In an offense involving unlawfully accessing, or exceeding authorized access to, a protected computer as defined in 18 U.S.C. § 1030(e)(2)(A) or (B) loss includes the reasonable cost to the victim of conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service.

delaying time-sensitive investigations. For example, if a DoS attack is launched on a California web site, but the attack originated in New York, was routed through a server in New Jersey, and bounced off a computer in Wisconsin on its way to California, investigators may be required to petition the court in each jurisdiction for an order to place a trace on the activity.[97] Under a new legislative proposal by Senators Charles Schumer and Jon Kyl, the federal government would unambiguously permit federal jurisdiction as soon as the attack occurs, rather than waiting for the damage assessment.[98] Also, damage estimates below $5,000 will be treated as a misdemeanor, while damage above $5,000 will still be treated as a felony. Finally, proposed legislation specifies that the costs of responding to the attack, damage assessment costs, repair to the system and lost revenue from the interruption of service will be counted toward the $5,000 damage amount.[99] Under the present statute, the damage calculation method is unclear and there has been little judicial precedent to provide guidance for allowable damage factors.[100]

The fifth section, § 1030(a)(5), is the main anti-hacking subsection. Subsection 1030(a)(5)(A) applies to whomever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[101] The DoS and DDoS attacker would be liable under this subsection both to the "zombie" systems and to the targeted systems. The attacker causes the transmission of a program on the "zombie" system and intentionally causes damage. The attacker also causes the transmission of information, the packets, and code, the datagrams that intentionally cause damage. This subsection provides serious sentencing guidelines. A first-time conviction can subject the attacker to up to five years in prison for each occurrence. According to United States Sentencing Commission, "[i]f the defendant is convicted under 18 U.S.C. Section 1030 (a)(4) or (5), the minimum guideline

97. *See Internet Denial of Service Attacks and the Federal Response: Panel I Of A Joint Hearing Of Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the Senate Judiciary Comm.*, 106th Cong. (2000) [hereinafter *Denial of Service Attacks*] (statement of Charles E. Schumer, United States Senator, New York).

98. *See* Office of Charles E. Schumer, *Schumer Offers Legislative Package to Combat Online Hacking* (Feb. 16, 2000) <http://www.senate.gov/~schumer/html/schumer_offers_legislative_pac.html>.

99. *See id.*

100. *See id.*

101. 18 U.S.C.A. § 1030(a)(5)(A) (West Supp. 1999).

sentence, notwithstanding any other adjustment, shall be six months' imprisonment."[102]

Section 1030(a)(5)(B) prohibits unauthorized access that recklessly causes damage to a protected computer.[103] Violation of this subsection is also a felony. However, the standard of reckless disregard is below the intentional damage provided under § 1030(a)(5)(A). If the prosecutor can show that the damage was intentional, as all DoS and DDoS attacks are, then the reckless disregard is unnecessary.

Section 1030(a)(5)(C) covers negligent damage to a protected computer. There is almost no conceivable scenario where this subsection could be used. Congress intended to punish the activity of hackers who do not intend to harm the systems but accidentally cause harm to the computer in the process. To only punish intentional harm would condone hacking into systems as long as no harm was done to the system.[104] However, in DoS and DDoS attacks, there could be no other reason a person would plant a daemon on another computer, or launch a DoS attack against another computer. Perhaps it is feasible that a curious computer user would enter a large ping command for another computer without a full understanding of the consequences. However, such conduct would be more reckless than negligent.

The sixth section, § 1030(a)(6), is concerned with the unauthorized trafficking of computer passwords and is not relevant to DoS attacks. Likewise, § 1030(a)(7) covers extortion threats against computer or network owners. This subsection would only be invoked if the attacker threatened to launch a DoS attack against the victim unless the victim pays the attacker "any money or other thing of value."[105]

---

102. *United States Sentencing Commission, Sentencing Guidelines for United States Courts, Part II,* 63 Fed. Reg. 602 (1998), *available in* 1998 WL 1699.

103. 18 U.S.C.A. § 1030(a)(5)(B) (West Supp. 1999).

104. One group of commenators suggests that:

> [S]tate and federal governments should immediately decriminalize all forms of non-malicious hacking. Non-malicious hacking should be defined as obtaining unauthorized access to a protected computer without causing intentional or reckless damage. Successful incidents of unauthorized access should be presumed by law to be non-malicious if the actor makes a good-faith effort to report the incident to the proprietor of the accessed system immediately upon obtaining access.

Lee et al., *supra* note 2, at 882-83. However, it could be argued that such a recommendation is the equivalent of de-criminalizing breaking and entering into a store with non-malicious intent if the burglars make a good faith effort to tell the owner they broke into the store. *See id.*

105. Bruce, *supra* note 88. None of the eight major companies that were hit by the DDoS attacks in February have reported that they received extortion threats. *See id.*

8. DoS Summary

Denial of Service attacks represent a significant threat to the stability of our network infrastructure because of the inherent vulnerability in the TCP/IP 3-handshake reliable protocol. Successful prosecution of the perpetrators should raise the awareness that DoS and DDoS are very serious crimes with serious consequences. Also, system administrators are likely to collaborate in devising plans for rapid network response to thwart the source of the attacks. However, where the system administrator's carrot may be minimized damage to their systems, the stick may be potential tort liability for allowing their system to be used in an attack against another server.[106] The tort standard of negligence could be: would a "reasonably prudent system administrator" have allowed a hacker to place a DDoS daemon on his system, and "but for" his negligence, the targeted server would not have been overloaded without his contribution? If the "zombie" computers were held liable for negligent administration of their servers, this also may help secure the Internet against DDoS attacks. Finally, the CFAA provides for a civil action for those who suffer any damage or loss against someone who violates 18 U.S.C. § 1030(a). The laws are in place to address the issue. Unfortunately, the greatest impediment to prosecuting will continue to be technical difficulty of tracing the route of the attack back to the perpetrator.

B. Web Site Defacing and Malicious Interference: User Level and Root Level Hacks

There are several reasons why a hacker would seek to hack into a web site and change a web page.[107] Web site hackers range from teenage pranksters to foreign powers seeking intelligence, and everything in between. Increasingly, there is a divide between the "old school" and "new school" hackers.[108] The "old school" hackers are associated more with the "Hacker's Ethics," a text that has been available on hacking newsgroups for several years.[109] The rift

106. *See* Eric J. Sinrod & Bill Reilly, *Lessons of DoS Attacks*, UPSIDE TODAY, (Feb. 29, 2000) <http://www.upside.com/texis/mvm/story?id=38b6dcbe0>.

107. According to the Director of the NIPC, "[Hackers] sometimes crack into networks simply for the thrill of the challenge or for bragging rights in the hacker community. Recently, however, we have seen more cases of hacking for illicit financial gain or other malicious purposes." *Cyberattack Investigation, supra* note 25.

108. Robert Richardson, *Hackers: Devils or Saints?*, NETWORK, June 1997, at 62.

109. According to one hacker: "True hackers want to learn, or want to satisfy their curiosity, that's why they get into the system. To search around inside of a place the you've never been, to explore all the little nooks and crannies of a world so unlike the boring cess-pool

between the two schools is often referred to as the "Black Hats" against the "White Hats."[110] The "old school" hackers complain that the widespread availability of ready-to-hack software does not require the level of sophistication that hacking required ten years ago, creating more opportunities to maliciously hack into systems without an understanding of the impact. They argue that irresponsible hacking has led to a higher profile of the "hobby" and a wave of new criminal laws that punishes both non-malicious intrusions and malicious intrusions. The "new school" hackers assert that many of the "old school" hackers have "sold out" to corporations as security experts.[111]

For the purposes of our discussion, hacking techniques will be divided into three large areas based on the hacker's intent. We will primarily address damage caused by non-authorized persons, not insiders who exceed their authorization.[112] The first major section is web site defacing and malicious interference with a web site, excluding Denial of Service attacks.[113] The second major section is unauthorized access for information and financial gain.

Basic Hacking Techniques:

There are as many hacking techniques as there are hackers. One common technique that is technically not a "hacking" technique, but is nevertheless a criminal violation, is the "cookie" exploit. A cookie is simply an HTTP header that consists of a text-only string that gets entered into the "memory" of a browser. This string contains the domain, path, lifetime, and value of a variable that a web site sets. If the lifetime of this variable is longer than the time the user spends at that site, then this string is saved to file for future reference.[114] For example, when a person signs up with a password and user name on a web site, the user's identification information is placed on the user's computer in the form of a cookie. When the user revisits the web site, the web site recognizes the user so that the user does not have to re-enter identifying information. However, some older web browsers

---

[sic] we live in." Dissident, *supra* note 14.

110. *See generally* Ashley Dunn, *A Haute Commodity; Hacking, Er, Vulnerability Analysis, Is Big Business*, L.A. TIMES, Aug. 1, 1998, at D1, D3.

111. *See id.*

112. *See* 18 U.S.C.A. § 1030(a)(1)-(4); (5)(A) (West Supp. 1999) (including both persons who exceed their authorized access, as well as persons without authorization).

113. *See* discussion *supra* Part III.A.

114. *See* David Whalen, *The Unofficial Cookie FAQ*, Cookie Central (visited Mar. 5, 2000) <http://www.cookiecentral.com/faq/#1.1>.

allow remote sites to retrieve cookies that were not planted by them, enabling malicious web site operators to "steal" the cookie, effectively retrieving the username and password. For example, Buysellzone.com allows registered users to place ads and have access to the various classified ad centers on their server. However, the cookie on the user's computer holds the user's name and password in text format, not encrypted, so anyone with access to the user's cookie.txt file can access the user's account.[115]

Depending upon the purpose of the intrusion, the risk level the hacker is willing to assume, the type of server, the remote and local operating systems, and countless other variables, there is a different hacking technique that can be deployed. Rather than exploring the details of several different techniques, for the purposes of gaining enough knowledge to understand the applicable provisions in 18 U.S.C. § 1030(a), it should be adequate to walk the reader through two hypothetical hacks.[116]

Regardless of whether the hacker intends to deface a web site or steal information, the ultimate technical objective is to "get root." The "root level" is also often referred to as the "god" account, where the "god" account has access to the entire system.[117] The root level provides the hacker with the same permissions and privileges as the system administrator. If the hacker can "penetrate" to the root level, he will be able to, among countless other possibilities, change passwords, access files, change web site files, re-route server traffic, and steal credit card numbers if the server is reckless enough to store unencrypted credit card numbers on its site.[118] Once the hacker "gets root," he must eliminate traces of his intrusion—his digital footprints—so the system administrator is unaware of his access.

However, not all hacks require "root access" to damage or change files on the server. Our first example is a relatively unsophisticated hack that only requires access to a user's account on

115. Most cookies are encrypted so that the information that is collected by the company that placed it on your computer is not readable to anyone except the company who encrypted it. On the one hand, this provides a level of security that prevents others from obtaining that information. However, the computer user is also unable to know that type of information that is being collected. It is important to note that cookies are text files, and therefore can not support a virus or software code that can place malicious scripts on a individual's computer.

116. A few other details have been changed to give the reader an overview of the process, so as not to provide a guidebook on how to actually hack a web site.

117. *See* Appendix A.

118. *See* David L. Gripman, *The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 169-70 (1997).

the server. We will refer to this as a "user-level hack." The second example demonstrates a "root access" hack that is significantly more dangerous to the integrity of the machine, although the statutes do not make the distinction. According to 18 U.S.C. § 1030(a), "access" is not defined by the level of penetration. Breaching the system in any manner to obtain information, obtain something of value or cause damage is enough to trigger the statutory liability. For the terms of this paper, we will refer to this type of hack as a "root access hack."

One way to explain the difference between the two hacks is to compare them to a non-technical example—a hotel. On "hosted" web sites, where the user "rents" web space on another company's server, there are two different levels of access: that of the system administrator and that of the lessee. In a hotel, there are also two main levels of access: the hotel management and the hotel guest. A guest only has a key to access a room (user access), while management has keys to access all of the rooms, as well as the back office, front door and the storeroom (system administrator's root access). A hacker who is able to "get root" has access to the management's keys, thereby gaining full access to everything in the hotel. However, just because someone has the hotel's "all access" key, does not necessarily mean they can enter the restricted areas freely because there are security guards (system administrators) and security cameras (server access logs). The goal of the "root hacker" is to enter unnoticed, compromise the security, and depart the scene without leaving any traces of his visit.

1. Example of a User-level Hack

Hacker wants to access a computer to deface a web site that was developed using Microsoft FrontPage. Hacker employs a technique that exploits a "bug" in FrontPage web sites that use FrontPage server extensions.[119] The first thing that Hacker must address is how to prevent his access from being traced. There are many ways to hide

119. For example:

> The FrontPage Server Extensions are a set of programs on a Web server that let the [webmaster] administer, author, and browse a FrontPage-based Web—a structure containing all of the pages, images, subdirectories, and other files that make up a Web site.
>
> The Server Extensions use standard Web server extensions interfaces, such as CGI and ISAPI, and work with virtually all existing Web servers. This design allows the FrontPage Server Extensions to be ported easily to all popular hardware and software platforms for cross-platform, Web-server compatibility.

Configuring and Deploying Microsoft FrontPage 2000 Server Extensions, (Oct. 1998) <http://www.microsoft.com/technet/FrontPg/TechNote/fpserext.asp>.

the origination of the hack, such as spoofing.[120] In this case, because Hacker does not want the victim to be able to trace him back to his point of origin, Hacker uses a laptop computer and a converted telephone lineman's handset to tap into the outside box of a neighbor's house by connecting two alligator clips to the appropriate box terminals. Hacker conducts the attack in the daytime, when the owner of the phone is not home, and the network traffic on the target site is more active.[121]

The next objective is to ascertain the user name and password for the site's webmaster, or the lessee, so he can access the web files on the server.[122] Hacker dials into a free ISP located in another region of the country to complicate the multi-company tracing investigation. Once he is on-line, Hacker enters an exploitative URL address that contains the "service.pwd."[123] Most web sites that use FrontPage server extensions locate the service.pwd in a predictable directory. If the server administrator was careless in setting up the "chmod" command that tells the server who can do what in a directory, such as granting the owner, groups or the public to read, write and execute files within the directory, then Hacker will be able to read a string of text that looks like the following: "kathy:paB.1Mg4MB6MF."[124] Hacker can already determine that the webmaster's username is "kathy." Now all that Hacker has to do is add a few commands to the password string, insert the password string into a DES decrypting password cracker and viola, Hacker has the webmaster's password as well.[125] From there, Hacker downloads the web page he wants to deface, alters the web page with his favorite web editor, and uploads the file to the server and the web page is "owned."

Applicable Federal Criminal Statutes:

In the above scenario, Hacker has broken numerous laws. Hacker would be liable under 18 U.S.C. § 1029(a)(7) which prohibits

120. *See* discussion *supra* Part III.A.6.

121. However, he could also attack at night when the system administrator is more unlikely to be monitoring the site.

122. Web hosting companies provide space on their server for individuals and companies who wish to have a presence on the internet without the need to maintain their own servers.

123. An "exploitive URL" is a URL that contains a certain string of letters and numbers that instruct the receiving server to respond in an unauthorized manner.

124. All UNIX and Linux directories have an access level control called the CHMOD that determines the access level of different groups.

125. Data Encryption Standard (DES) is a relatively weak encryption technique that is often used to encrypt passwords on a system.

the knowing possession of a "telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services" with the intent to defraud.[126] Hacker modified the modem and the lineman's handset, also known as a "beige box."[127] Also, Hacker may be liable for a violation of 18 U.S.C. § 1343, which prohibits the intentional scheming to obtain "money or property by means of false or fraudulent pretenses" by "wire."[128] In *United States v. Freeman*,[129] the court held that the use of a "blue box" to bypass long distance charges is a taking of property under § 1343. Hacker intentionally schemed to take "property" from the phone company or the victim whose phone line he tapped with the telephone lineman's handset. A violation of the subsection carries a prison term of not more than five years.[130]

One of the difficulties prosecutors face with many of the subsections under § 1030(a) is the requirement for "damage," which is defined as a loss aggregating at least $5,000 in value during a one year period.[131] If only the text of a web page is altered in the attack, and the system is not "damaged," then meeting the $5,000 threshold may be difficult. The subsections that penalize only the "access" with no damage requirement, § 1030(a)(1)-(3), have an easier burden to meet. However, unless the hacker has broken into a computer that contains restricted data;[132] has received information valued at more than $5,000;[133] committed acts in the furtherance of another criminal

---

126. 18 U.S.C.A. § 1029(a)(7) (West Supp. 1999).

127. According to the Jargon Dictionary, "phreaking" is the:

> [A]rt and science of cracking the phone network (so as, for example, to make free long-distance calls)....
>
> ... There was significant crossover between the hacker community and the hard-core phone phreaks who ran semi-underground networks of their own through such media as the legendary "TAP Newsletter." This ethos began to break down in the mid-1980s as wider dissemination of the techniques put them in the hands of less responsible phreaks. Around the same time, changes in the phone network made old-style technical ingenuity less effective as a way of hacking it, so phreaking came to depend more on overtly criminal acts such as stealing phone-card numbers....

The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/p.html#phreaking>.

128. 18 U.S.C § 1343 (1994).

129. 524 F.2d 337 (7th Cir. 1975).

130. *See* 18 U.S.C § 1343 (1994).

131. *See* 18 U.S.C.A. § 1030(e)(8)(A) (West Supp. 1999).

132. *See id.* § 1030(a)(1).

133. *See id.* § 1030(c)(2)(B)(iii).

or tortious act;[134] or committed acts for commercial or private financial gain,[135] the crime is only a misdemeanor. The three subsections that measure a threshold value of at least $5,000 for information, anything of value, or damage, are often difficult to prove in the type of hack explained above.[136]

If the web site that Hacker altered was located on a computer that is used by or for the government of the United States, then he could be liable for a misdemeanor violation of 18 U.S.C. § 1030(a)(3), which criminalizes the intentional access of such non-public computers.[137]

Hacker could be charged with a misdemeanor violation of 18 U.S.C. § 1030(a)(2)(C), which protects any information intentionally obtained from a protected computer. The "information" he obtained would be the web site owner's user name and password, along with any other information he may have viewed. The courts have held that "accessing" of information is not limited to taking the information. "Access" applies to the "intent" to access, not the "intent" to damage the protected computer.[138] Viewing the information on the computer is considered "access." In other words, the *mens rea* for this crime is the intent to access the computer and there is no requirement for the actual transport of the information. Also, if Hacker defaced the web site with a "url redirect" to his own company's web site, then the charge could be bumped up to a felony for those acts considered for commercial advantage or private financial gain.[139]

Prosecutors may be able to charge Hacker with a violation of 18 U.S.C. § 1030(a)(4) if they can show he obtained something of value worth more than $5,000 or § 1030(a)(5) if they can show Hacker caused $5,000 or more damage.[140]

---

134. *See id.* at (ii).

135. *See id.* at (i).

136. Section 1030(a)(4) uses a $5,000 damage threshold. Section 1030(a)(2) violations are misdemeanors unless the access was for personal gain, the value exceeded $5,000, or they were committed in furtherance of another crime.

137. *See* 18 U.S.C.A. § 1030(a)(3) (West Supp. 1999).

138. *See* United States v. Sablan, 92 F.3d 865, 867 (9th Cir. 1996).

139. *See* 18 U.S.C.A. § 1030(c)(2)(B)(i) (West Supp. 1999).

140. Please note that Hacker would still be liable for any state anti-hacking statutes even if the federal government was unable to meet the statutory threshold for Federal jurisdiction. However, a discussion of state statutes is beyond the scope of this article. The definition of "damage" under 18 U.S.C. § 1030 (in addition to the $5,000 threshold), includes any impairment to the integrity of a protected computer that modifies or impairs the medical examination, diagnosis or care of one or more individuals, *see* 18 U.S.C.A. § 1030(e)(8)(B) (West Supp. 1999); causes physical injury to any person, *see id.* at (C); or threatens public health or safety, *see id.* at (D). In this scenario, none of these other definitions of "damage" are

Under § 1030(a)(4), merely viewing the information may not meet the statute's definition of "obtaining" information.[141] Congress intended to punish the theft of information, not merely punish unauthorized access.[142] In *United States v. Czubinski*, an Internal Revenue Service employee was charged with the unauthorized access of confidential income tax records. However, the court found that he only viewed the information and did not use the information in any manner. The First Circuit Court of Appeals held that the information obtained "is the showing of some additional end—to which the unauthorized access is a means—that is lacking here."[143] However, in Hacker's case, he did use the user information he obtained as a means to the additional end of hacking the web site.

2. Example of a "Root-Access" Hack

The objective of this hack is to obtain a higher system privilege than in a user-level attack, or in other words, to get the manager's "all access" keys. The first part of the hack entails getting access to the password files. The second part is cracking the password or taking advantage of a server "bug" that will allow access to the more privileged "root" level. Once at the "root" level, the hacking goal can be achieved, whether it is planting a Trojan,[144] obtaining sensitive files, downloading the system password files, stealing stored unencrypted credit card numbers, etc. The third part of the hack is covering the intrusion tracks and installing a "backdoor" that will allow future access. In this part, the system logs are modified to remove traces of the attack. Once these three steps have been achieved, the hacker is considered to "own" the system.

Hacker targets a system he wants to "own," a small business ISP that offers web site space on its server. On the ISP's system is a small company web site that sells products over the Internet and stores credit card information on the web site in a weakly encrypted form. Hacker also wants to plant a Tribe Flood Network daemon on the site.[145]

The first thing Hacker does is to sign on for a trial "shell"[146]

---

likely.

141. *See* United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

142. *See id.*

143. *Id.*

144. *See* discussion *infra* Part III.C.3.

145. *See* discussion *supra* Part III.A.5.b.

146. *See* Appendix A.

account under an assumed identity with the ISP. With shell access, Hacker telnets into his shell account and enters a series of commands that exploit a "Sendmail" program.[147] Due to the "hole" in the Sendmail program, the telnet commands write a message directly to the "/etc/passwd" directory that gives Hacker a password-free root account. However, this exploit could leave several traces and may not grant him the complete access he needs to steal the credit cards, although he should be able to plant the daemon. Once he has root access, his next objective is to download the system's passwords so he can log on as another user, reducing his chances of being caught.

After Hacker has downloaded the systems passwords, he has to decipher them. After a user has created a password, the password is scrambled in an algorithm to generate a "one-way hash."[148] This requires extensive computer processing power. Many password crackers hack into more power computers to run the cracking programs. Congress specifically intended to apply 18 U.S.C. § 1030(4) to the use of another's computer processing power. Senator Jon Kyl noted during Senate discussion of the National Information Infrastructure Protection Act of 1996 that the bill:

> [A]mends 18 U.S.C. § 1030(a)(4) to ensure that felony-level sanctions apply when unauthorized use, or use in excess of authorization, is significant. Hackers, for example, have broken into computers only for the purpose of using their processing programs, sometimes amassing computer time worth far more than $5,000. The bill would penalize those whose trespassing, in which only computer use is obtained, amounts to greater than $5,000 during any one year period. Companies should not be stuck with the bill for electronic joyriders. Although they may not damage or

147. Sendmail is a freeware program that many systems use to handle e-mail assignments. This exploit is for an older version of send mail and was patched several years ago. Although it is beyond the scope of the article to give specific hacking techniques, a non-specific demonstration of the process should be adequate to provide the elements for a statutory analysis. *See* United States v. Morris, 928 F.2d. 504, 506 (2nd Cir. 1991) (Robert Morris describes a Sendmail exploit as one of the methods he used to launch his worm program.).

148. Most servers do not "decrypt" a password when a user enters a password on a site. Instead, the password is run through the algorithm to generate a one-way hash. If the hash matches the hash that is associated with the user name, then the password is valid. The passwords that Hacker downloaded were really just "hashes." Hacker must run the passwords through a password "cracker," which is a program that runs words and number combinations through known algorithms continuously until a match with the stolen password appears. The word that generated the matching algorithm is the password. The most common password cracking techniques are Dictionary Crackers and Brute Force Crackers. A Dictionary Cracker runs a database of words through the algorithms one a time until a match is found. A Brute Force Cracker runs every possible combination of words and letters together until the password is found.

> steal information, hackers who browse through computer systems are a significant liability to businesses who must pay for a new security system, and the expensive time the hacker used.[149]

After Hacker has cracked the password, he will log into the small business' account by File Transfer Protocol (FTP), go to the directory where the credit card numbers are stored and download the files. However, his access to the directory will be logged somewhere by the system administrator. Hacker must either use his root account, or any other password to edit the log files. Hacker will try to determine if there is anyone else on the system. If the system is clear, Hacker would explore the system to find where the log files are stored and uses a "rootkit" that will automate the sweeping up of intrusion by replacing several critical files.[150] Hacker will create a "hidden" directory on the server that will enable the directory to avoid detection with a standard Linux "ls" command which shows a list of directories in a given path.[151]

Hacker will then hide the "rootkit" in the hidden directory. In addition, if Hacker wants to continue to "own" the site for future access, he can leave a "backdoor" on the system in a modified binary that will enable him to bypass the current, and possibly any future security measures.[152] In this case, Hacker will place a Trojan program in the /bin/login/ directory under a specific user name configured for telnet logins so he can re-enter the system with the minimum amount of attention. In addition, Hacker could plant a "sniffer" that will capture all network traffic, including the user names, passwords, and credit card information. The "sniffer" will log all of the activity in a file for Hacker to retrieve at a later time. After Hacker is ready to wind up his hacking intrusion, he will initiate the "Trojan binaries" to wipe the log files and log off of the system.

Applicable Federal Criminal Statutes:

In a "root access" hack, the potential for serious crime escalates because of the information that can be obtained, the damage that can be caused, and the value of data obtained. One way to analyze

149. *National Information Infrastructure Protection Act of 1996: Hearings on S. 982,* 104th Cong. 90 (1996) [hereinafter *Hearings on S. 982*] (statement of United States Senator Jon Kyl, United States Senetor, Arizona).

150. *See* Lance Spitzner, *They Gain Root, Know Your Enemy: III* (last modified Aug. 13, 1999) <http://www.enteract.com/~lspitz/enemy3.html>.

151. *See id.*

152. *See id.*

§ 1030(a) is to first look at the type of computer that was targeted. If the computer was a federal government computer or a computer used by or for the federal government, then § 1030(a)(1)-(3) could apply. However, in the example above, Hacker most likely targeted a private ISP computer. The next step in the analysis is to determine if the hacker obtained information,[153] obtained anything more than $5,000 in value,[154] or damaged the protected computer.[155] At the point when Hacker exploited a hole in the Sendmail program, he did not obtain any information, nor did he arguably obtain anything of value, or do over $5,000 damage to the computer at this point.

However, Hacker's next move, downloading the password files, is clearly obtaining information under 18 U.S.C. § 1030(a)(2)(C) and Hacker is liable for a misdemeanor unless the prosecution can show that the value exceeds $5,000, was for personal gain, or was committed in furtherance of another crime.[156] Section 1030(a)(2)(3) was meant to protect privacy where the value of the information, although lacking quantifiable monetary value, is nevertheless valuable in terms of privacy. Also, during congressional hearings on the CFAA, Senator Leahy noted that if:

> [T]he information obtained is of minimal value, the penalty is only a misdemeanor. If, on the other hand, the offense is committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000, the penalty is a felony."[157]

If Hacker downloaded an entire batch of passwords, the prosecution may be able to argue that the aggregate value of the web site's security was more than $5,000, triggering § 1030(a)(4) liability.

Hacker's theft and possession of the credit card numbers is a violation of several statutes. First, Hacker could be liable under 15 U.S.C. § 1644(b), which proscribes the transport of stolen credit cards. In *United States v. Callihan*,[158] the court held that the defendant did not "transport" the credit card when he gave the credit

153. 18 U.S.C.A. § 1030(a)(2)(C) (West Supp. 1999).

154. *See id.* § 1030(a)(4).

155. *See id.* at (5).

156. *See id.* § 1030(c)(2)(B).

157. *Hearings on S. 982, supra* note 149 (statement of Patrick Leahy, United States Senator, Vermont).

158. 666 F.2d 422, 424 (9th Cir. 1982).

card number over the phone. The court concluded that the numbers by themselves did not meet the statutory language of "credit card," which "as used in section 1644 means the small, flat tablet upon which a credit card account number is imprinted, but does not mean that number alone."[159] However, a year later, in *United States v. Bice-Bey*,[160] another court held that an individual who orders goods with a fictitious name by telephone, using credit card numbers without the authorization of card holders, although she did not have cards in her possession, nevertheless violated 15 U.S.C. § 1644(a), since a core element of a credit card is the number, which can be used over telephone without seller ever seeing the plastic card itself. Although the *Bice-Bey* decision concerned the "use" of the credit card, the court still held that the credit card numbers transferred over the phone constituted a violation of § 1644(a).

Also, Hacker most likely violated 18 U.S.C. § 1029(a)(3) if he obtained more than fifteen credit card numbers.[161] Section 1029(a)(3) states that it is a punishable offense to "knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices."[162]

According to 18 U.S.C. § 1029(e)(1), an "access device" means:

> [A]ny card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.[163]

If Hacker uses one of the credit cards, he will have violated 18 U.S.C. § 1029(a)(2), if he "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value

159. *Id.*

160. 701 F.2d 1086, 1092 (4th Cir. 1983).

161. In 1997, Carlos Salgado hacked into several companies and ISPs by using a packet sniffer that collected user log on information. Mr. Salgado obtained a list of thousands of credit cards and was caught when he attempted to sell them on a CD-ROM to an undercover FBI agent at the San Francisco International Airport. He subsequently pleaded guilty to four counts: two counts of computer crime under 18 U.S.C. § 1030, and two counts of trafficking in stolen credit cards under 18 U.S.C. § 1029. *See* Richard Power & Rik Farrow, *Electronic Commerce Crime; Includes Related Article on Excerpt from a Hacker's E-mail; Internet/Web/Online Service Information*, NETWORK, Dec. 1997.

162. 18 U.S.C.A. § 1029(a)(3) (West Supp. 1999).

163. *Id.* § 1030(e)(1).

aggregating $ 1,000 or more during that period."[164] If Hacker is found guilty of violating § 1029(a)(2) or (3), he can be sent to prison for up to ten years.[165]

When Hacker edited the log files to cover his intrusion, he caused damage to the computer under 18 U.S.C. § 1030(a)(5)(C), which criminalizes the intentional damage of a computer. His alteration of the log files resulted in reckless or negligent damage, as provided for under § 1030(a)(5)((B)-(C)). Hacker also violated the same subsection when he created a hidden directory and planted the backdoor. When Hacker installed the sniffer to intercept the network traffic, he damaged the system in violation of § 1030(a)(5)(A), possibly violated § 1030(a)(4) if he obtained anything of value from the "eavesdropping," and most likely violated § 1030 (a)(3)(C) by obtaining information from a protected computer and violated the privacy that Congress specifically intended to protect.[166]

As one can see from the above hacking examples, the hacking technique used in an attack will determine which of the subsections are relevant for both criminal and civil actions.[167]

C. Malicious Code - Viruses, Worms, and Trojans

Malicious code is computer code that is written with the sole intent to cause damage to a machine or to invade the machine to steal information. The most common forms of malicious code are viruses, worms, and Trojan programs. Some of these forms may share similar techniques or objectives. However, there are substantial differences between the various forms and different federal laws may apply to each form, depending on the technical method in which the offending code damages the victim.

1. Viruses

Viruses have become a serious financial and security threat to computer networks across the world.[168] According to CERT, there are an estimated 30,000 computer viruses in existence today and there are

164. *See* 18 U.S.C.A. § 1029(c)(1)(A)(i), § 1029(a)(2) (West Supp. 1999).

165. *See id.* § 1029(c)(1)(A)(i).

166. *Hearings on S. 982, supra* note 149.

167. Incidentally, 18 U.S.C.A. § 1030(g) (West Supp. 1999) allows a victim to maintain a civil action against the violator to obtain compensatory or other equitable relief.

168. *See The Melissa Virus: Hearing of the Technology Subcomm. of the House Science Comm.*, 106th Cong. (1999) [*hereinafter Melissa Virus Hearings*] (statement of Michael A. Vatis, Director, NIPC, Federal Bureau of Investigation).

approximately 300 new viruses created each month.[169]

A virus is a program than infects a computer by inserting a copy of itself into the computer and harms the computer in some manner, generally without the computer user's awareness.[170] Not all viruses cause damage to its host. Viruses that are "benign," or non-harmful, are still considered viruses. For example, a virus could display an innocuous message on a certain date. Although it might be annoying and create a sense of anxiousness, the virus does not cause any measurable harm. However, the current anti-virus and anti-hacking statutes[171] do not always distinguish between harmful and benign viruses.[172]

A virus is typically spread from one computer (computer A) to another (computer B) by e-mail or an infected disk. However, the virus on computer B does not infect the computer until the program is "executed." A common method of virus execution is when computer B's user is tricked into opening a file attached to an e-mail, thinking the file is a harmless program coming from a friendly source. However, recent viruses, such as Bubbleboy, can infect a computer when a user merely reads an e-mail, without opening any attachments.[173]

A virus can also be executed by hiding a "macro" routine in a

---

169. *See id.* The CERT Coordination Center is part of the Survivable Systems Initiative at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. CERT was started by DARPA (the Defense Applied Research Projects Agency, part of the U.S. Department of Defense) in December 1988 after the Morris Worm incident crippled approximately 10% of all computers connected to the Internet.

170. *See Introduction to Computer Viruses*, Sophos Virus Info (May 26, 1998) <http://www.sophos.com/virusinfo/articles/virusintro.html>.

171. 18 U.S.C.A. § 1030 (West Supp. 1999).

172. *See* 18 U.S.C.A. § 1030(a)(4)-(5) (West Supp. 1999) (stating that a virus must cause "damage,"or the hacker must obtain "something of value").

173. According to Symantec:

> VBS.BubbleBoy is a worm that works under Windows 98 and Windows 2000. The worm will also work under Windows 95 only if the Windows Scripting Host is installed. The worm will only work with the English and Spanish versions of the operating systems, and not with Windows NT. Microsoft Outlook (or Express) with Internet Explorer 5 must be used in order for the worm to propagate. The worm utilizes a known security hole in Microsoft Outlook/IE5 to insert a script file, *UPDATE.HTA*, when the email is viewed. It is not necessary to detach and run an attachment. *UPDATE.HTA* is placed in Program-StartUp of the Start menu. Therefore, the infection routine is not executed until the next time you start your computer.

Symantec AntiVirus Research Center, *VBS.BubbleBoy* (visited Mar. 4, 2000) <http://www.symantec.com/avcenter/venc/data/vbs.bubbleboy.html> [hereinafter *VBS.BubbleBoy*].

common Microsoft Office product file, like Word or Excel, and the macro can command the computer to act in harmful ways.[174] Files that contain only data, such as image files (.gif and .jpg), music files (.wav and .mp3) and text files that do not contain macro functionality (.txt) are not capable of transmitting a virus because they cannot command the computer to perform any functions.[175]

Once a virus is activated, it does not have to cause damage immediately. There are countless creative ways a virus can be triggered.[176] Most viruses contain a "payload," which contains the damaging code.[177] The "payload" is the damage a virus creates.[178] In the past, virus payloads have been triggered on a certain date,[179] when the computer re-starts,[180] or after a certain amount of times the virus is loaded into the system.[181] Viruses can hide in several places in a computer's memory.[182] Other viruses hide in computer programs so that the virus is activated every time the program is loaded.[183] Once the virus is activated, it can duplicate and spread itself without any further input by the user.[184]

Once a virus is loaded onto the hard drive[185] and "launches" its

174. *See* Richard Raysman & Peter Brown, *Viruses, Worms, and Other Destructive Forces,* N.Y.L.J., July 13, 1999.

175. *See id.*

176. For example, a virus payload can be triggered to cause damage to a machine on a certain date; by launching an infected executable file; by running a companion program; or after the user enters a certain word in a program. *See id.*

177. *See id.*

178. *See id.*

179. *See* Symantec AntiVirus Research Center, *W95.LoveSong.998* (visited Mar. 4, 2000) <http://www.symantec.com/avcenter/vinfodb.html> [hereinafter *W95.LoveSong.998*].

180. *See VBS.BubbleBoy, supra* note 173.

181. *Id.*

182. *See* Raysman & Brown, *supra* note 174.

183. *See id.*

184. *See id.*

185. A hard disk, or memory, is the main memory where programs and the operating system are permanently stored. As an example, one can think of the hard drive as a large filing cabinet, the random access memory (RAM) as a table, and the processor as a clerk. When the clerk wants to work on a file, he goes to the filing cabinet and brings the file to the table, where he can open up the file and read it. If the clerk wants to read another file, he repeats the process. The relationship between the hard drive, RAM, and processor can be further illustrated by adjusting the variables. If a lot more filing cabinets are added, but the size of the desk is still the same, the clerk will not be able to increase the number of files he can put on the table. If the size of the desk is increased, but the clerk moves slowly, then too many files on the desk may actually slow him down. The operating system is the set of instructions that coordinate all of the actions that take place in the computer. Although operating systems often come on CD-ROMs, they are not "computer programs." A program can only run "on top of an operating system." The operating system is like the translator that gets all of the hardware and software talking

payload, the results can range from annoyingly humorous like "W95.LoveSong.998," which causes a Korean love song to play on a certain date[186] to total devastation like "the Emperor," which will permanently overwrite data on the hard disk and then attempt to destroy the Flash BIOS.[187] There is also concern that a macro virus placed on a government computer could e-mail sensitive or classified material to others without the knowledge of the computer's user.[188]

a. The Melissa Virus

The Melissa Macro Virus was launched in March, 1999 and rapidly spread through computers across the world. The Melissa Macro Virus was a virus that was hidden in a Microsoft Word attachment that appeared to come from a person known to the recipient. When the attachment was opened, a list of pornographic web site passwords were displayed. However, unknown to the user, the program also activated a macro that read the first fifty e-mail addresses located in the Microsoft Outlook e-mail program and e-mailed itself to the fifty addresses with the message subject header "Important Message from (the name of someone on the list)."[189] The virus was estimated to have caused $80 million in damages and spread so quickly that within 48 hours, Microsoft and Intel were forced to shut down their servers.[190] One company reported that its "500-employee computer network was buffeted by 32,000 e-mail messages in a 45 minute period, effectively shutting it down for

---

together. In the above example, the operating system is like the employee handbook that tells the clerk what he is supposed to do and how he is supposed to do it. Many viruses hide in the boot sector area of the hard disk that the operating system checks when it begins to load the operating system.

186. *See W95.LoveSong.998, supra* note 179.

187. *See* Symantec AntiVirus Research Center, *Emperor* (visited Apr. 9, 2000) <http://www.symantec.com/avcenter/venc/data/emperor.html> [hereinafter *Emperor*].

> A computer's basic input-output system (BIOS) is typically a read-only memory (ROM) that is programmed at the time it is manufactured with particular low-level code responsible for basic boot functions and managing persistent data such as the date and time. Most recent PCs have been manufactured with a relatively new type of memory called *Flash* ROM. BIOS in Flash ROM is often referred to as Flash BIOS. Flash BIOS capability means that enhancements can be installed using a special program without having to physically replace a chip.

Mitre (visited Mar. 31, 2000) <http://www.mitre.org/research/cots/FLASHBIOS.html>.

188. *See Melissa Virus Hearings, supra* note 168 (statement of Michael Vatis, Director, NIPC, Federal Bureau of Investigation).

189. Raysman & Brown, *supra* note 174.

190. *See ZDTV Exclusive: Accused Author of Melissa Computer Virus to Plead Guilty in Court Tomorrow*, PR NEWSWIRE, Dec. 8, 1999.

legitimate purposes."[191]

The author of the virus, David Smith, was quickly caught and pled guilty to state[192] and federal charges. Mr. Smith pled guilty to intentionally causing damage to computers, 18 U.S.C. § 1030(a)(2), (5)(A), with an admission that he was responsible for the $80 million in damages that affected over a million computers.[193] The Melissa Macro Virus resulted in the first successful prosecution of a virus writer in over a decade[194] and only the second successful prosecution in history,[195] despite the fact that viruses continue to plague the Internet.[196]

Applicable Federal Criminal Statutes:

The relevant and tested federal anti-virus statutes are 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1030(a)(2). If a virus is loaded into a computer by an e-mail attachment, and the author intended to cause "damage" to the recipient computer, then 18 U.S.C. § 1030(a)(5)(A) is applicable. Section 1030(a)(5)(A) prohibits the knowing transmission of a program, code, or command, that results in intentional damage without authorization to a protected computer.

If the virus author did not intend to cause damage to the computer, but rather the code accidentally damaged the computer as a result of the e-mail transmission, then as an alternative to the above statute, the author may be prosecuted under 18 U.S.C. § 1030(a)(5)(B) which covers reckless damage to a computer as a result of unauthorized and intentional access. The penalties for both § 1030(a)(5)(A) and (B) are the same—up to five years in prison. A negligence standard would be considered too low for an intentional act, as provided by 18 U.S.C. § 1030(a)(5)(C), which is a misdemeanor.

If the recipient of the virus forwards the virus on to another

---

191. *Melissa Virus Hearings, supra* note 168.

192. Mr. Smith plead guilty to second-degree computer theft under N.J.S.A. 2C:20-25. *See Cyberattack Investigation, supra* note 25.

193. *Cyberattack Investigation, supra* note 25.

194. *Denial of Service Attacks, supra* note 97.

195. *See id.*

196. One of the most common viruses in 1999 and 2000 is another Microsoft Word Macro virus called WM97/Marker. *See Sophos Virus Info* (visited Mar. 14, 2000) <http://www.sophos.com/virusinfo/topten/>. This virus sends a message to an Internet site containing the File Information Summary whenever the window is closed. *See id.* Although this information may not be highly sensitive, it could only be the beginning of significant invasions of privacy on the Internet by viruses.

person via e-mail, then his mental state, or *mens rea*, will determine his culpability.[197] If he is unaware that there is a virus, then he will not have the requisite mental state.[198] If he is aware that there is a virus, then he could face § 1030(a)(5)(A) liability because he intentionally sent the virus.[199] However, if he was aware there was a virus attached to the e-mail, but he thought it was a harmless prank, for example, then his act could be reckless or negligent; mental states that can trigger § 1030(a)(5) sanctions.

There is a possibility that a virus may not reach federal jurisdiction if the virus was transmitted to a stand-alone computer by diskette. Section 1030(a)(5) covers only "protected computers," those that are "used in interstate or foreign commerce or communication."[200] If the computer has a modem or a fax server loaded on it, then the prosecution could argue that it is a protected computer because it is a computer "which is used in interstate or foreign commerce or communication."[201] However, if the virus is loaded onto a non-networked computer that, for example, is used in a small office for billing and the virus is placed on it by a diskette, a strong argument can be made that it is not a protected computer under federal jurisdiction because it is not a computer "which is used in interstate or foreign commerce or communication."[202]

However, if the virus is loaded onto a computer and causes any of the enumerated damages in § 1030(e)(8), then action against the attacker might be brought under the statute. For example, if the virus was loaded onto a computer that was used to store medical records, and if the virus impaired the treatment or care of an individual because the patient's medical records were destroyed, then it would trigger criminal liability even though the damage did not meet the monetary threshold.[203] Of course, there are state anti-virus laws which would bring the attack under state jurisdiction if federal jurisdiction is unavailable. However, a discussion of state statutes are beyond the scope of this article.

Section 1030(a)(2) has been successfully used against viruses that have invaded the system and sent information from the

197. *See* Haeji Hong, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 296 (1997).

198. *See id.*

199. *See id.*

200. 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 1999).

201. *Id.* § 1030(e)(2)(A).

202. *Id.*

203. *Id.* § 1030(e)(2)(8).

computer.[204] Section 1030(a)(2)(C) criminalizes the intentional access of a computer without, or in excess of authorization, to obtain information from any protected computer if the conduct involved interstate or foreign commerce. In this case, it is irrelevant if the virus was loaded into the computer by a diskette because the e-mailing of the information, such as Melissa's fifty e-mail contacts, invokes federal jurisdiction because it involves interstate and foreign commerce.

Finally, if the e-mail attachments made their way to a Federal Government computer or a computer that "is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States," then the sender of the virus could be liable for a misdemeanor under § 1030(a)(3).[205]

If a Melissa Macro-type virus were to infect a Government computer, then the virus sender could be liable under § 1030(a)(2)(B), which prohibits the intentional access of a computer and obtaining information from the Federal Government. The e-mail addresses in Microsoft Outlook could be considered "information." However, if any information that is considered protected against unauthorized disclosure "for reasons of national defense or foreign relations, or any restricted data," then the virus sender could be liable under § 1030(a)'s most serious violation—§ 1030(a)(1). This subsection provides for a prison term up to ten years.

2. Worms

Worms are similar to viruses. However, one major distinction is that worms multiply without any human interaction. A worm can wind its way through a network system without the need to be attached to a file, unlike viruses.[206]

The Haiku worm is a good example of a robust worm with many features. The Haiku worm spreads itself through e-mail with an attachment called "haiku.exe." When the worm is executed, it modifies the system to load every time the computer is re-booted. After the computer is re-booted, a small haiku poem will appear in a window box. The worm generates it own haikus from a list of words. The worm will also search the hard drive for e-mail addresses and the worm will send haiku.exe with a message to the e-mail addressees it

204. *See* Wendy Davis, *Prosecutors Watching the Web Street Crime is Down, but that may Just Mean it's Moving Online,* 158 N.J. L.J. 933 (1999).

205. 18 U.S.C.A. § 1030(e)(2)(8) (West Supp. 1999).

206. *See* Raysman & Brown, *supra* note 174.

located on the hard drive.[207] However, although the worm is annoying, it is not malicious.

a. The Morris Worm

Robert Morris was a first-year graduate student in Cornell University's computer science Ph.D. program when he released a computer worm with the intent to demonstrate the vulnerability of computers to malicious programs. He programmed the worm to multiply only once on a computer, thereby helping the worm evade detection. However, to defeat system administrators who might trick the worm into thinking the computer already had the worm, Morris designed the worm to automatically reproduce every seventh time, regardless of whether the machine already had the worm. However, Morris underestimated the number of iterations the worm would make. The worm multiplied across the Internet much more quickly than anticipated and he made attempts to limit the damage by releasing a solution over the Internet. However, due to network congestion caused by the worm, the solution was not able to get through until serious damage had already been done to many protected computers across the country. The estimated cost to repair each infected installation ranged from $200 to more than $53,000. Morris was charged with violating 18 U.S.C. § 1030(a)(5)(A). The trial court convicted Morris and the Second Circuit upheld the conviction on grounds that § 1030(a)(5)(A) "does not require the Government to demonstrate that the defendant intentionally prevented authorized use and thereby caused loss."[208] In 1996, Congress codified the *Morris* court's holding by specifying the levels of *mens rea* required for three subsections of § 1030(a)(5), two felony and one misdemeanor.

Applicable Federal Criminal Laws:

As some worms multiply exponentially and wind their way through the Internet, they can cause extensive damage in overloaded servers and anti-worm extraction. If a company has 500 computers on a network that become infected, the cost to extract the worms would easily meet the $5,000 threshold for damages. As Congress

207. Symantec AntiVirus Research Center, *W95.Haiku.16384.Worm* (visited Apr. 6, 2000) <http://www.symantec.com/region/uk/avcenter/venc/w95_haiku_16384_worm.html> [hereinafter *W95.Haiku.16384.Worm*].

208. United States v. Morris, 928 F.2d 504, 505 (2nd Cir. 1991).

learned after the *Morris* case, the intent to access,[209] not the intent to damage, has to be the standard as the world becomes more interconnected.[210]

If a worm is received by a user and executed and installed in the system, § 1030(a)(5)(C) would cover the knowing transmission of that program if it caused an aggregate $5,000 in damage. Sections 1030(a)(5)(B)-(C) may not be available because of the non-targeted nature of worms. Those subsections proscribe the "intentional access" of protected computers and a worm is indiscriminately sent out, at least after the first wave. Likewise, nothing of value is taken[211] and no information is obtained,[212] so the other subsections will not be relevant in a standard self-replicating worm program.

3. Trojan Horse Programs

A Trojan Horse program, or Trojan program, is an innocent-looking program that contains hidden functions. They are loaded onto the computer's hard drive and executed along with the regular program. However, hidden in the belly of the "innocent" program is a sub-program that will perform a function, mostly unknown to the user. Trojan programs can take the form of a popular program where the original source code has been altered to hide the Trojan "payload."

a. Back Orifice 2000

Back Orifice 2000 (BO2K) is a Trojan program that is designed for misuse and attack on another computer. It is an advanced program that takes a group of complex hacking and networking activities and bundles them into one graphical interface. The hacker has the victim install the "server" on his computer without his knowledge, typically in the form of an e-mail attachment. After the victim has loaded the BO2K on his machine, the hacker is able to gather information on the victim's computer, perform system commands, redirect network traffic and reconfigure the victim's computer. The damage that a hacker can do to a computer is limitless, and the invasion of privacy could cause serious damage to companies and individuals. BO2K invisibly resides on the remote

209. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. *See id.* at 506.

210. *See* Hatcher et al., *supra* note 1, at 406-07.

211. 18 U.S.C.A. § 1030(a)(4) (West Supp. 1999).

212. *See id.* at (1)-(3).

victim's computer and can perform unauthorized actions without the user's knowledge. If the victim is on a network, the hacker could gain broad access to that network.[213]

The installation of BO2K involves installing the client on the hacker's computer and getting the victim to install the server on his machine. Once BO2K has been properly configured, the server sitting on the victim's computer silently waits for instructions from the hacker's client. BO2K has over seventy commands that it can send from the hacker's client to the server. The hacker simply has to scroll down a list of commands, click on the command he wants to initiate on the remote server, and push the "Send Command" button. The server's response will appear in a window below the command list.[214] The solution to these Trojan programs is to avoid opening e-mail attachments, particularly from non-trusted sources. In addition, all of the major anti-virus detection kits can locate BO2K software on computers.

Applicable Federal Criminal Laws:

Trojan programs are specifically the type of computer crimes § 1030(a) was meant to address because the likelihood of malicious damage that can cause millions of dollars in damages is very high. As the economy becomes more inter-networked, the risks posed by programs such as BO2K are increasing.

Like virus distribution, if the Trojan program writer gives a program on a diskette to someone who installs the program on a stand-alone computer, and the computer is damaged, there may not be adequate Federal jurisdiction in this scenario. The computer may not be considered a "protected computer" that is "used in interstate or

213. BO2K can be analogized to receiving a package that contains a hidden microphone.

214. The following are examples of BO2K Commands: System commands, including the ability to shut down and reboot the remote computer, freeze up the remote computer and retrieve a list of the user names and passwords located on the machine; Key Logging commands enable the hacker to send each keystroke the victim makes to a text file on the victim's computer, where he can later retrieve the keystroke log file with the click of a button. Keyloggers are the most pernicious of privacy invasions because the keystroke logger saves every key pressed on the keyboard, eliminating the possibility of erasing your thoughts or later encrypting them because the hacker has access to every letter you typed before you erased the documents or encrypted it; MS Networking commands allows the hacker to access other computers on a local network; Registry commands enables the hacker to edit the computer's registry, the virtual "guts" of the computer system; Multimedia Commands permits the hacker to capture video stills and play .wav files located on the remote computer; File/Directory commands provide the hacker with the ability to view the directory list, and find, view, copy and delete files. Obviously, this type of silent access on a computer is a severe invasion of privacy. *See* BO2K Docs (visited Apr. 7, 2000) <http://www.bo2k.com/docs/cmdrefindexbar.html>.

foreign commerce or communication."[215]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the "payload" is harmless, it may be difficult to establish "damage" under § 1030(a)(4) or § 1030(a)(5). According to § 1030(e)(8), "damage" is defined as any "impairment to the integrity or availability of data, a program, a system or information that (A) causes a loss aggregating at least $5,000 in value during any 1-year period or one or more individuals."[216]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the "payload" *does* cause damage, and if the "damage" definition in § 1030(e)(8) can be met, then the program author would at least be liable under § 1030(a)(5)(A), which prohibits the knowing transmission of a program, information, code, or command that intentionally causes damage. If the Trojan program makes its way onto several computers, the damage calculation could be met more easily due to § 1030(e)(8)'s damage definition that includes "one or more individuals."[217]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the Trojan program is a program similar to Back Orifice that transmits information from the victim's computer to another computer, then there are several statutes that could apply to the Trojan writer's actions, depending on the computer that was infected.

If the computer infected by a BO2K-type Trojan was a private person or company, then the hacker would be liable under § 1030(a)(2), which prohibits obtaining information from the intentional unauthorized access of a protected computer. Here, there is no damage threshold. However, this crime is presently only a misdemeanor, unless the value of the information exceeds $5,000 or it was committed in the furtherance of another crime, in which case it is bumped up to a felony.

Under the same scenario, the hacker would also be liable under § 1030(a)(5)(A), which prohibits the knowing transmission of a program or command that intentionally causes damage to a protected computer. Once again, the damage threshold is an aggregate $5,000 in any one year period to one or more individuals. If this burden can

215. 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 1999).

216. *Id.* § 1030(e)(8).

217. *Id.*

be met, then the hacker is subject to up to five years in prison.

Theoretically, under this scenario, the Trojan program writer could be liable under § 1030(a)(4). That subsection covers the knowing intent to defraud a protected computer and the procurement of anything of value in excess of $5,000. This is a felony crime. Nonetheless, Congress did not want to make a felony out of every hacker that breaks into a computer and uses its processing power, for example, and does not obtain anything of value.[218]

The hacker could be liable under the more serious § 1030(a)(1) and subject to ten years in prison if the hacker's BO2K Trojan ends up on any computer containing information that is protected by a national statute, or restricted data that could be considered to be used to the injury of the United States, or to the advantage of any foreign nation. The delivery element is met because even if the information is not transferred to the hacker's client computer, there is a provision in the subsection for an attempted transmission.

IV. NEW COMPUTER CRIME LEGISLATION

Senators Charles Schumer and Jon Kyl have introduced new legislation, S. 2092, aimed at addressing some of the perceived weaknesses in the CFAA. The three main provisions addressed by this new legislation propose the following: trap and trace orders, federal jurisdiction requirements, and sentencing.[219]

First, the new legislation would make it easier for cyber-investigators to obtain "trap and trace" orders. "Trap and trace" devices are used to capture incoming IP packets to identify the packet's origins. Due to the ease with which hackers are able to "spoof" their true origin, the most effective way to reconstruct the path of a virus, DoS, or hacking assault is to follow a chain of trapping devices that logged the original malicious packets as they arrive at each individual router or server. In the case of a single telephone company, it has been relatively easy for investigators to obtain trap and trace orders.[220] According to Congresswoman Scott of Virginia, "one communication is being carried by several different [ISPs], by a telephone company or two, local or long distance, by a cell company or two, and soon enough by a satellite company or two."[221] Once the segment of the route goes beyond the court's

218. *See* Hatcher et al., *supra* note 1, at 407.

219. *See Trap and Trace, supra* note 89.

220. *See id.*

221. *Id.*

jurisdiction, investigators must then go to the next jurisdiction and file a request for a trap and trace order for the next segment. The new legislation would authorize the issuance of a single order to completely trace an on-line communication from start to finish.[222]

The second provision would lower the monetary barrier for federal jurisdiction. Currently, the CFAA requires a damage threshold in excess of $5,000.[223] However, the $5,000 threshold is often difficult to establish when there is no fixed monetary value to the information. Also, investigators must currently wait for a damage assessment before they can initiate an investigation, which can cause expensive delays. The new legislation would permit federal jurisdiction at the outset of an attack. Crimes that exceed $5,000 will still be treated as felonies.[224] However, attacks that cause less than $5,000 in damage would be defined as misdemeanors. Finally, the legislation clarifies what is included in the calculation of "damage," making it easy to reach the $5,000 threshold.[225] It provides for the costs of responding to the offense, the damage assessment costs, restoration costs, and any lost revenue or costs incurred from the interruption of service.[226]

The third provision would modify the strict sentence directives contained in the Antiterrorism and Effective Death Penalty Act of 1999 which required a mandatory incarceration for a minimum of six months for any violation of 18 U.S.C. § 1030(a).[227] Some hacking crimes have gone unprosecuted because the six month sentence was considered excessive. The new legislation would provide lesser sentences for lesser crimes, helping to ensure that all levels of hacking cases will be prosecuted.[228]

Finally, the proposed legislation would make juvenile perpetrators fifteen years of age and older eligible for federal prosecution in serious computer crime cases at the Attorney General's discretion.[229]

However, the proposed changes have raised privacy concerns. A report written by the President's Working Group on Unlawful Conduct on the Internet entitled "The Electronic Frontier: the

222. *See id.*
223. *See* S. 2092 IS, 106th Cong. §2 (2000).
224. *See id.*
225. *See id.*
226. *See id.*
227. *See id.*
228. *See id.*
229. *See* S. 2092 IS, 106th Cong. §2 (2000).

Challenge of Unlawful Conduct Involving the Use of the Internet" has raised the concerns of privacy advocates.[230] The groups are particularly concerned about the potential for trap and trace abuse by authorities.[231] The American Civil Liberties Union (ACLU), would like to raise the standards for trap and trace devices, rather than lower them.[232] According to the ACLU, law enforcement currently only needs to overcome "minimum obstacles" to obtain trap and trace devices.[233] The ACLU is concerned that an expansion of the government's power to obtain trap and trace orders will enhance the government's power to "surreptitiously intercept even more personal electronic communications."[234] The current standard for a trap and trace order is that the investigator must assert in writing to the court that the information is "relevant" to an ongoing investigation.[235] According to the ACLU, the "judge to whom the application is made *must* approve the application, *even if he disagrees* with the assertions of law enforcement."[236]

Additionally, the ACLU is concerned that an expansion of the substance of the orders will erode privacy. The ACLU speculates that an expansion of the powers "might allow law enforcement agents to access a variety of data, including dial-up numbers, IP addresses, electronic mail logs, uploaded files, and so on.... without a court order."[237]

The CFAA is broad enough to cover most computer crimes. The Act protects government and private computers against inside and outside threats to information, fraud, and damage. Continued pro-active legislative changes to keep the Act up to date in the escalating cyber-war between secure web sites and hackers will be critical to maintaining the integrity of our increasingly inter-networked society. One challenge in the near future will be the expansion of the number of devices that are able to access the Internet. For example, as televisions become "web-enabled," allowing users to access the

230. Robyn E. Bumner, *Government Wants to Bore Web Peephole*, ST. PETERSBURG TIMES, Mar. 12, 2000, at 4D.

231. *See, e.g.*, letter from Barry Steinhardt, Associate Director, ACLU, to Janet Reno, Attorney General of the United States (Mar. 8, 2000) (on file with the *Santa Clara Computer and High Technology Law Journal*).

232. *See id.*

233. *See id.*

234. *Id.*

235. *See id.*

236. *Id.*

237. Letter from Barry Steinhardt, *supra* note 231.

Internet from their televisions, will televisions be considered "high-speed data processing devices" as defined under the Act's "computer" definition? Would passwords taken from the television's cookie storage be protected under the Act? As Wireless Application Protocol (WAP) brings the Internet to hand-held devices and mobile telephones, will the devices and telephones be considered "protected computers"?

Cyber-crime prosecutors are also facing the difficulty of attacks that originate overseas beyond their jurisdiction. If part of a hacking trail is routed overseas, unless the U.S has an agreement with the foreign jurisdiction, that trail could lead to a dead end if investigators do not have access to the server's logs. The world of individual national jurisdictions will need to address the increasingly borderless crimes committed in cyberspace. However, the CFAA provides a solid foundation upon which we can develop new cyber-crime laws for the coming century.

V. CONCLUSION

Over the course of the past ten years, cyber-crimes have progressed from being malicious pranks by disenchanted teenagers to a serious threat that will tax the resources of crime enforcement and potentially destabilize society. Successful criminal prosecution and civil litigation will require that members of the legal community familiarize themselves with the various hacking techniques to ensure that the perpetrators are tried and convicted under the relevant statutes. A misapplication of the law to a specific hacking technique could allow a hacker to walk free. Likewise, members of the business community must understand the serious risks associated with conducting business on-line and their responsibility to the other companies for negligent maintenance of their systems.

And finally, hackers who naively believe in their right to access information, must be made aware that even harmless computer intrusions can trigger criminal sanctions. The financial stakes have risen dramatically over the past five years. Until there are more high profile hacking prosecutions, naïve hackers will continue to believe that they are invulnerable and their hacks are a form of innocent digital thrill seeking. Nevertheless, over the next few years, there will be a few hackers whose only hacking and cracking is going to be breaking rocks on a chain gang.

APPENDIX A

The following definitions are taken from the Jargon Dictionary: *The Jargon File, version 4.2.0,* available on-line at <http://www.netmeg.net/jargon/>.

cracker *n.* One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker []. An earlier attempt to establish 'worm' in this sense around 1981-82 on Usenet was largely a failure.

Use of both these neologisms reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings. While it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past larval stage is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done).

Thus, there is far less overlap between hackerdom and crackerdom than the mundane reader misled by sensationalistic journalism might expect. Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open poly-culture this lexicon describes; though crackers often like to describe *themselves* as hackers, most true hackers consider them a separate and lower form of life.

Ethical considerations aside, hackers figure that anyone who can't imagine a more interesting way to play with their computers than breaking into someone else's has to be pretty losing [sic].

daemon */day'mn/ or /dee'mn/ n.* [from the mythological meaning, later rationalized as the acronym 'Disk And Execution MONitor'] A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The idea is that the perpetrator of the condition need not be aware that a daemon is lurking (though often a program will commit an action only because it knows that it will implicitly invoke a daemon). For example, under ITS writing a file on the LPT spooler's directory would invoke the spooling daemon, which would then print the file. The advantage is that programs wanting (in this example) files printed need neither compete for access to nor understand any idiosyncrasies of the LPT. They simply enter their implicit requests and let the daemon decide what to do with them. Daemons are usually spawned automatically

by the system, and may either live forever or be regenerated at intervals.

Daemon and demon are often used interchangeably, but seem to have distinct connotations. The term 'daemon' was introduced to computing by CTSS people (who pronounced it /dee'mon/) and used it to refer to what ITS called a dragon; the prototype was a program called DAEMON that automatically made tape backups of the file system. Although the meaning and the pronunciation have drifted, we think this glossary reflects current (2000) usage.

FTP */F-T-P/, not* /fit'ip/ **1.** *[techspeak]* n. The File Transfer Protocol for transmitting files between systems on the Internet. **2.** vt. To beam a file using the File Transfer Protocol. **3.** Sometimes used as a generic even for file transfers not using FTP. "Lemme get a copy of "Wuthering Heights" ftp'd from uunet."

hacker *n.* [originally, someone who makes furniture with an axe] **1.** A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. **2.** One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. **3.** A person capable of appreciating hack value, which is defined as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a hack. **4.** A person who is good at programming quickly. **5.** An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) **6.** An expert or enthusiast of any kind. One might be an astronomy hacker, for example. **7.** One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. **8.** *[deprecated]* A malicious meddler who tries to discover sensitive information by poking around. Hence 'password hacker', 'network hacker'. The correct term for this sense is cracker. . . .

root *n. [Unix]* **1.** The "superuser" account (with user name 'root') that ignores permission bits, user number 0 on a Unix system. The term avatar is also used. **2.** The top node of the system directory structure; historically the home directory of the root user, but probably named after the root of an (inverted) tree. **3.** By extension,

the privileged system-maintenance login on any OS. . . .

server *n.* A kind of daemon that performs a service for the requester and which often runs on a computer other than the one on which the server runs. A particularly common term on the Internet, which is rife with 'web servers,' 'name servers,' 'domain servers,' 'news servers,' 'finger servers,' and the like.

shell *[orig. Multics n.* techspeak, widely propagated via Unix] **1.** *[techspeak]* The command interpreter used to pass commands to an operating system; so called because it is the part of the operating system that interfaces with the outside world. **2.** More generally, any interface program that mediates access to a special resource or server for convenience, efficiency, or security reasons; for this meaning, the usage is usually 'a shell around' whatever. This sort of program is also called a 'wrapper.' . . .

TCP/IP */T'C-P I'P/ n.* **1.** [Transmission Control Protocol/Internet Protocol] The wide-area-networking protocol that makes the Internet work, and the only one most hackers can speak the name of without laughing or retching. Unlike such allegedly 'standard' competitors such as X.25, DECnet, and the ISO 7-layer stack, TCP/IP evolved primarily by actually being *used,* rather than being handed down from on high by a vendor or a heavily-politicized standards committee. Consequently, it (a) works, (b) actually promotes cheap cross-platform connectivity, and (c) annoys the hell out of corporate and governmental empire-builders everywhere. Hackers value all three of these properties. . . .

TELNET */tel'net/ vt.* (also commonly lowercased as 'telnet') To communicate with another Internet host using the TELNET [] protocol (usually using a program of the same name). TOPS-10 people used the word IMPCOM, since that was the program name for them. Sometimes abbreviated to TN /T-N/. "I usually TN over to SAIL just to read the AP News."

I KNOW IT WHEN I SEE IT: SHOULD INTERNET PROVIDERS RECOGNIZE COPYRIGHT VIOLATION WHEN THEY SEE IT?

Irina Y. Dmitrieva[†]

TABLE OF CONTENTS

I. INTRODUCTION

Internet service providers (ISPs) are gateways to the world of cyberspace. They provide on-line access to individuals, educational institutions, corporations, and government agencies. At the same time, they can easily "pull the plug" on cyber-speech by taking down

[†] Irina Y. Dmitrieva is a Ph.D./J.D. candidate at the University of Florida at Gainesville. The author would like to thank Professors Bill Chamberlin and Thomas Cotter, University of Florida, for their helpful comments, and Professor Donald Gillmor, University of Minnesota, for sparking my initial interest in copyright law.

questionable material and terminating the accounts of specific users. In this sense, ISPs have become on-line guardians of free speech. ISPs, however, should not become Internet censors or decision makers on what constitutes copyright violations on the Internet.

For example, fans of Homer J. Simpson may put his images on their personal web sites.[1] Likewise, those who enjoy novels of Iris Murdoch[2] may quote her extensively on their web pages. Most Internet users also hope that on-line services will notice their sites and list them in their Internet directories, so that more people could visit them. Fans believe that the fair use provision of copyright law protects their use of copyrighted images or excerpts from the novels. However, the owners of copyrights for the famous cartoon series or Iris Murdoch's novels may think otherwise. In this situation, when compilers of Internet directories come across such fan sites, should they decide whether the sites violate copyright law? And if a compiler decides that a violation occurred, should it immediately block access to the site?

The Online Copyright Infringement Liability Limitation Act (OCILLA) signed into law in October 1998,[3] provides that ISPs are required to expeditiously take down on-line material when they become "aware of facts or circumstances from which infringing activity is apparent."[4] The issue is: Just how "apparent" a copyright infringement should be for a service provider to take restrictive actions against it? In other words, should ISPs be expected to know a copyright violation when they see it?

This article argues that in light of the OCILLA's legislative history, courts should narrowly construe the new "awareness" standard. If courts broadly interpret this requirement, ISPs may have incentive to restrict more on-line material than necessary without fear of being punished, because the same law shields them from liability for taking down, in good faith, allegedly infringing content.[5] Part I of this paper provides an overview of the ISPs' liability in copyright infringement suits before the passage of the statute. Part II

1. Homer Simpson is a leading character of the popular FOX animation series, The Simpsons. Fan sites include The Simpsons Archive at <http://www.snpp.com>, Evergreen Terrace at <http://www.milpool.com>, and The Simpsons Channel at <http://simpsons.lardlad.com>.

2. Iris Murdoch is a famous 20th century British novelist.

3. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, Tit. II, 105th Cong. (1998).

4. 17 U.S.C.A. § 512(c)(1)(ii) and (d)(1)(B) (West Supp. 1999).

5. *See* id. § 512(g)(1).

summarizes the main provisions of the OCILLA. Part III describes the legislative history of the statute, with particular focus on drafting the new knowledge and awareness requirement. Finally, Part IV argues for the narrow judicial interpretation of the new awareness standard in light of the statute's language, structure, and legislative history.

A. Liability of ISPs for Copyright Violations of Their Users Before the OCILLA

Copyright law provides economic incentives for authors to engage in creative activities by granting them a temporary monopoly over their works.[6] Exclusive rights of copyright owners include the rights to reproduction, distribution, display and performance, and the right to prepare derivative works.[7] To better ensure financial remuneration of authors, copyright law imposes strict liability[8] for copyright violations. This means that an individual's intentions and knowledge are irrelevant in determining whether a copyright violation occurred. Courts find individuals strictly liable even for innocent copyright violations.[9]

Strict liability principles of copyright law differ dramatically from the liability principles in defamation and obscenity law, where courts take into consideration the element of knowledge (*scienter*) on the part of a defendant.[10] Defamation and obscenity laws distinguish between primary publishers and distributors, with the latter subject to a more lenient standard of liability.[11] On the contrary, under copyright law, distributors such as bookstores may be found strictly

---

6. U.S. CONST. art.1, § 8, cl. 8.

7. *See* 17 U.S.C. § 106 (1994).

8. The concept of liability is defined as "every kind of legal obligation, responsibility, or duty;" "condition of being responsible for a possible or actual loss, penalty, evil, expense, or burden." BLACK'S LAW DICTIONARY 914 (6th ed. 1990).

9. However, courts may consider the innocent character of a violation in assessing punitive damages.

10. See for example *Smith v. California*, 361 U.S. 147, 149-50 (1959), where the Supreme Court invalidated on First Amendment grounds a Los Angeles city ordinance which imposed strict criminal liability on a retail bookseller for possession of an obscene book. The Court held that the ordinance, which did not consider the element of *scienter* (distributor's knowledge of the contents of a book), inhibited freedom of expression by forcing booksellers to inspect the contents of all reading materials they carry.

11. See for example *Cubby, Inc. v. Compuserve*, 776 F. Supp. 135, 139-40 (S.D.N.Y. 1991), where the New York federal district court found a service provider not liable for allegedly defamatory statements posted by its independent contractor, because, the court said, Compuserve performed the role of a traditional news vendor.

liable for unauthorized distribution of infringing materials.[12]

Courts base responsibility for copyright violations on three theories of liability: Direct, vicarious, and contributory. Direct and vicarious liability are examples of strict liability, which do not take into consideration the element of knowledge. Direct infringement occurs when an individual violates one of the exclusive rights of a copyright owner. For example, direct violation occurs when a vendor distributes bootleg recordings, or when a person reproduces a copyrighted work without the author's permission.

Vicarious liability is imposed on an individual or entity that does not commit a copyright violation, but directly benefits from it and has the right and ability to control it. Vicarious liability is an outgrowth of the doctrine of *respondeat superior*, according to which a master is responsible in certain cases for the wrongful acts of his servants. For example, a dance hall owner may be found vicariously liable for leasing his premises to a band that performs copyrighted songs without permission.[13]

The only theory of liability that considers the element of knowledge on the part of an infringer is contributory liability. Contributory liability is an outgrowth of a common law principle that those who knowingly participate in the act of direct infringement should be held accountable for their wrongful actions. To be found contributorily liable, a person "must have acted with the direct infringer and must have known of the infringing activity."[14] For example, an operator of a retail copy service may be found contributorily liable for helping his customers copy protected audiotapes by using his cassette recorder.[15]

With the development of the Internet, the question arose as to which standard of liability should apply to ISPs. Two federal district court decisions framed the debate on this issue. In the 1993 case, *Playboy Enterprises, Inc. v. Frena*,[16] a Florida federal court ruled that

12. 17 U.S.C. § 106(3) (1994) grants copyright owners the exclusive right to distribute copies of their works to the public. The distribution right applies to all copies of copyrighted works, whether or not they were lawfully made. *See* NIMMER ON COPYRIGHT § 8.11. The distribution right is limited by the "first sale" doctrine. Under 17 U.S.C. § 109 (1994), a lawful owner of a particular copy of a copyrighted work can sell or otherwise dispose of that copy without the copyright owner's permission.

13. *See* Dreamland Ball Room v. Shapiro, Bernstein & Co., 36 F.2d. 354, 355 (7th Cir. 1929).

14. PAUL GOLDSTEIN, COPYRIGHT § 6:1 at 6.6 (2d ed. 1999).

15. *See* RCA Records v. All-Fast Systems, Inc., 594 F. Supp. 335, 340 (S.D.N.Y. 1984).

16. 839 F. Supp. 1552, 1559 (M.D. Fla. 1993).

a computer bulletin board (BBS) operator was directly liable for illegal materials posted to his system by subscribers. The court ignored the fact that the BBS operator claimed he did not know about copyright violations on his system, and, as soon as he learned about them, he took down the infringing materials. This decision alarmed the ISP community which said that imposition of strict liability on service providers would compel them to monitor private transmissions of their users in effort to detect potential copyright violations.[17] By monitoring transmissions of their subscribers, ISPs risk violating another federal law, the Electronic Communications Privacy Act, which prohibits interference with private digital communications, such as electronic mail.[18]

In the 1995 case, *Religious Technology Center v. Netcom Online Communications*,[19] a federal court in California refused to follow Florida's precedent in holding an ISP strictly liable for copyright violations of its users. Instead, the court ruled that liability of ISPs should be based on the theory of contributory infringement. Under this theory, liability for participation in illegal activity is established when the defendant, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[20] The California court's decision received fire from the community of copyright owners who argued that, by introducing the element of knowledge into the liability scheme, the court encouraged ISPs to turn a blind eye on copyright violations on their networks.[21]

The debate over the proper copyright liability standard for ISPs unfolded in academic circles. Most of the research on this issue appeared in law reviews. For example, Jane Ginsburg of Columbia University School of Law argued that ISPs should be subject to the strict liability standard because they facilitate transmissions of

17. "Absent clear lines of liability, service providers may have no practical defense to crippling damages but the invasive monitoring and supervision of their subscribers' private communications." *NII Copyright Protection Act of 1995: Hearing on S. 1284 Before the Senate Comm. on the Judiciary*, 104th Cong. 48 (1996) (statement of Robert Oakley, Digital Future Coalition).

18. *See* H.R. REP. NO. 105-551, Pt. 1, at 26 (1998) (stressing that the new statute does not require ISPs to access, remove or disable access to material if in violation of the Electronic Communications Privacy Act).

19. 907 F. Supp. 1361 (N.D. Cal. 1995).

20. Gershwin Publ'g Corp. v. Columbia Artists Management Corp., 443 F.2d 1159, 1162 (2d Cir. 1971), *quoted in* Religious Tech. Ctr., 907 F. Supp. at 1382.

21. *NII Copyright Protection Act of 1995 (Pt. 2): Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong. 35-38 (1996) (statement of Edward M. Murphy, National Music Publishers' Association).

infringing messages.[22] Ginsburg also wrote that copyright owners may choose to sue a bulletin board or commercial network operator as a "profitable intermediary" to recover some of their losses from copyright violations.[23]

Others stressed that if ISPs are exposed to strict liability, they would start monitoring transmissions on their networks, thus turning into on-line censors. Law professor Niva Elkin-Koren wrote that imposition of strict liability on ISPs is not a sound policy choice because it would turn ISPs into inspectors, or supervisors of the on-line information flow.[24] Pamela Samuelson of the University of California at Berkeley also warned against ISPs becoming "centralized control centers to enforce copyright law."[25]

Some scholars noted that under existing case law, ISPs can be held vicariously and contributorily liable for activities of their users. For example, Mary Ann Shulman wrote that ISPs who reap advertisement revenue when users hit their web sites might be found liable if the content includes infringing material.[26]

Several scholars came to the conclusion that courts should hold ISPs accountable for acts of their users only if copyright owners can demonstrate that ISPs had actual knowledge of copyright violations. For example, Giorgio Bovenzi wrote that the appropriate standard of liability for ISPs is negligence under the actual knowledge requirement.[27] According to Bovenzi, the actual knowledge requirement would ensure the freedom of on-line communications because ISPs would not have the incentive to monitor transmissions of their users for potentially infringing content.[28] Bovenzi suggested that upon receipt of a complaint from a copyright owner, ISPs should be required to remove an allegedly illegal message.[29]

---

22. *See* Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1492-94 (1995).

23. *See id.* at 1499.

24. *See* Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 410 (1995).

25. Pamela Samuelson, *The Copyright Grab*, WIRED, Jan. 1996, at 190.

26. *See* Mary Ann Shulman, Comment, *Internet Copyright Infringement Liability: Is an Online Access Provider More Like a Landlord or a Dance Hall Operator?*, 27 GOLDEN GATE U. L. REV. 555, 599 (1997).

27. *See* Giorgio Bovenzi, *Liabilities of System Operators on the Internet*, 11 BERKELEY TECH. L.J. 93, 141 (1996). The article is available at (visited Mar. 15, 2000) <http://www.law.berkeley.edu/journals/btlj/articles/11_1/Bovenzi/html/reader.html>.

28. *See id.* at 139.

29. *See id.* at 140; *see also* Wendy Melone, Note, *Contributory Liability for Access*

Unfortunately, neither case law nor academic commentary provided a consistent solution to the problems of ISPs' liability for copyright violations of their users. The answers to some of those questions came in October 1998, when Congress enacted limitations on copyright liability for ISPs as part of the Digital Millennium Copyright Act.

B. Summary of Key Statutory Provisions

Congress passed the Online Copyright Infringement Liability Limitation Act (OCILLA)[30] as Title II of the Digital Millennium Copyright Act,[31] signed into law by President Clinton on October 28, 1998. OCILLA, which took effect on the same date, amended Chapter 5 of the Digital Millennium Copyright Act by adding a new section called "Limitations on liability relating to material online."[32]

OCILLA applies to ISPs and nonprofit institutions of higher education in their capacity as service providers.[33] It creates a number of "safe harbors" for service providers against liability for copyright violations of their users, based on the functions performed by service providers. The liability limitations apply to four general categories of activity: Transitory digital network communications,[34] system caching,[35] storage of information residing on systems or networks at

---

Providers: Solving the Conundrum Digitalization Has Placed on Copyright Laws, 49 FED. COMM. L.J. 491, 506 (1997) (suggesting that copyright owners should be required to notify ISPs of copyright violations on their networks).

30. Digital Millennium Copyright Act, Pub. L. No. 105-304, Tit. II, 105th Cong (1998).

31. Digital Millennium Copyright Act, Pub. L. No. 105-304, 105th Cong. (1998).

32. 17 U.S.C.A. § 512 (West Supp. 1999).

33. The term "service provider" is generally defined as "a provider of online services or network access, or the operator of facilities thereof." *Id.* § 512(k)(1)(B). For example, this broad definition would include providers of Internet access, commercial on-line services, and operators of individual computer bulletin boards (BBS).

OCILLA also provides an additional, more narrow definition of a service provider which applies only to the subsection covering transitory digital network communications. For the purposes of this subsection, a service provider is defined as "an entity offering the transmission, routing, or providing of connections for digital on-line communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." *Id.* § 512(k)(1)(A). In order to qualify for this definition, a service provider must perform a passive role of a conduit—for instance, to provide e-mail service, or mailing lists (Listserv).

34. The concept of "transitory digital network communications" describes the process of "moving packets of information across digital online networks," such as forwarding e-mail traffic or routing messages to a mailing list agent (Listserv). COMM. ON THE JUDICIARY HOUSE OF REPRESENTATIVES, 105th Cong., 2d Sess., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 26 (Comm. Print Serial No.6 1998).

35. System caching is a technique employed by ISPs to speed up public access to popular

the direction of users,[36] and information location tools.[37] These "safe harbors" protect service providers from all monetary relief for direct, contributory, and vicarious infringement, and substantially limit injunctive relief against qualifying service providers.

To be eligible for liability limitations, service providers shall designate an agent to receive notifications of copyright violations on their networks[38] and shall implement a policy for the termination of accounts of those subscribers who repeatedly violate copyright.[39] In addition, service providers should not interfere with "standard technical measures" used by copyright owners to identify and protect their works.[40] This provision reflects the belief of members of Congress that, in the future, technology may provide solutions to many issues facing copyright owners.[41] The statute specifies that "standard technical measures" should be developed by both copyright owners and ISPs in "an open, fair, voluntary, multi-industry standards process."[42] For example, members of the House Committee on Commerce anticipated that organizations such as the World Wide Web Consortium, the Internet Engineering Task Force, or ad hoc

---

web sites. When a user requests access to a certain web site, a local Internet server automatically makes a temporary copy of the requested file. This is done in case other users from the same area would want to visit this particular site. In this case, they will access it from the local server instead of re-calling the site from possibly thousands of miles away. See *Information Resource Caching FAQ* (visited Feb. 5, 2000) <http://www.ircache.net/Cache/FAQ>.

36. "Examples of such storage include providing server space for a user's web page, for a chatroom, or other forums in which material may be posted at the direction of users." COMM. ON THE JUDICIARY HOUSE OF REPRESENTATIVES, 105th Cong., 2d Sess., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 26 (Comm. Print Serial No.6 1998).

37. The term "information location tools" refers to directories of on-line sites, search engines, lists of recommended sites, hyperlinks. *See id.* at 32.

38. 17 U.S.C.A. § 512(c)(2) (West Supp. 1999).

39. *See id.* § 512(i)(1)(A). Members of the House Committee on Commerce described the goals of a copyright policy in the following way: "[T]hose who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access." *See also* Digital Millennium Copyright Act of 1998, *Report on H.R. 2281 of the House Comm. on Commerce*, Rept. 105-551, Pt. 2, 105th Cong., 2d Sess., at 61 (1998).

40. *See* 17 U.S.C.A. § 512(i)(1)(B) (West Supp. 1999).

41. *See Report on H.R. 2281 of the House Comm. on Commerce*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 61 (1998); *see also* COMM. ON THE JUDICIARY HOUSE OF REPRESENTATIVES, 105th Cong. 2d Sess., SECTION-BY-SECTION ANALYSIS OF H.R.2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 26, at 37 (Comm. Print Serial No.6 1998) (stressing that technology is likely to provide solutions to many issues facing copyright owners and ISPs).

42. 17 U.S.C.A. § 512(i)(2)(A) (West Supp. 1999).

industry groups, could take an active part in this process.[43]

OCILLA essentially creates a series of affirmative defenses for service providers who are found liable for copyright violations under existing principles of law.[44] At the same time, if service providers fail to qualify for liability limitations under OCILLA, they still can assert other defenses available under copyright law, such as the fair use defense.[45]

Subsection (a) of OCILLA limits liability of service providers who perform only a passive "conduit" function in the process of transmitting, routing, or providing connections for digital communications of others. This provision resembles the "passive carrier" exemption of the Copyright Act.[46] Under section 111(a)(3) of the Copyright Act, certain "passive carriers" are exempt from copyright liability as long as they do not directly or indirectly control the content of their transmissions and clientele.[47] Traditionally, the passive carrier exemption has applied to communications common carriers regulated by the Federal Communications Commission. Examples of "passive" functions performed by ISPs include provision of e-mail services, newsgroups, and listserv services.

For a service provider to qualify for the "conduit" limitation, several conditions must be met: A service provider must not initiate, select or modify the content of the communication; it must not determine the recipients of the message, or maintain a copy of the message on a system or network in a manner ordinarily accessible to other people for a longer period than is reasonably necessary for the transmission.[48]

Subsection (b) of OCILLA limits liability of service providers for intermediate storage of material in the process of system caching,

---

43. *See Report on H.R. 2281 of the House Committee on Commerce*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 61-62 (1998).

44. *See Report on H.R. 2281 of the House Comm. on the Judiciary*, Rept. 105-551, Pt. 1, 105th Cong. 2d Sess., at 26 (1998) ("[T]he exemption and limitations provided in this subsection are affirmative defenses, like the exceptions and limitations established elsewhere in title 17.").

45. *See* 17 U.S.C.A. § 512(l) (West Supp. 1999).

46. *See Report on H.R. 2281 of the House Comm. on Commerce*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 63 (1998) (stressing that the definition of a service provider for purposes of subsection (a) reflected the fact that the "functions covered by new subsection (a) are essentially conduit-only functions").

47. 17 U.S.C.A. § 111(a)(3) (West Supp. 1999) (stating that activities of passive carriers should be limited to "providing wires, cables, or other communications channels for the use of others").

48. *See id.* § 512(a)(1-5).

under certain conditions. These conditions include: no modification of the material's content by a service provider; regular updating of the material in accordance with accepted technical standards; no interference with the ability of technology to return certain data to the original site; and no circumvention of password mechanisms.[49] In addition, a service provider shall expeditiously remove the material claimed to be infringing upon notification from a copyright owner.[50]

The other two functions protected by the liability limitations—information residing on a system or network at the direction of users and information location tools—contain conditions that combine the elements of contributory and vicarious liability. Subsection (c) applies to activities such as provision of server space for users' web pages or chat forums.[51] Subsection (d) applies to the on-line navigational tools, such as search engines, hypertext links, Internet directories, and lists.[52]

Both subsections establish a new knowledge standard for finding the service providers' liability. They provide that ISPs shall not be liable for third-party copyright violations if ISPs do not have actual knowledge that the material or activity on their networks is infringing, or, in the absence of such knowledge, are not "aware of facts or circumstances from which infringing activity is apparent."[53] The statute requires that, upon obtaining such knowledge or awareness, a service provider must act expeditiously in removing the allegedly infringing material off-line. In addition, to avoid liability, a service provider shall not receive a financial benefit directly attributable to the infringing activity.

OCILLA establishes a somewhat different standard of knowledge for nonprofit educational institutions in their capacity as service providers. Subsection (e), inserted by the House and Senate conference committee, provides that when a faculty member or graduate student performs a teaching or research function, such faculty or student's knowledge of infringing activities, generally, shall not be imputed to an institution.[54] Exceptions to this rule include situations when infringing materials were officially required or recommended for a class taught at an institution for the preceding

49. *See id.* § 512(b)(2).
50. *See id.* § 512(b)(2)(E).
51. *See id.* § 512(c).
52. *See id.* § 512(d).
53. 17 U.S.C.A. § 512(c)(1)(ii) and (d)(1)(B) (West Supp. 1999).
54. *See id.* § 512(e).

three years; and when the institution received more than two notifications of copyright violations within three years but failed to act on them. In addition, institutions are required to implement a copyright policy and to promote compliance with it.

OCILLA sets forth the rules for the "notice and take-down" procedure,[55] which provides that copyright owners may notify an ISP of alleged copyright violations on the ISP's networks. Upon receipt of such notification, an ISP is expected to "take down" or disable access to the allegedly infringing material. The statute requires that effective notification shall identify allegedly infringing works, and provide information that would permit service providers to locate an infringing site and to contact a copyright owner.[56] In addition, the notification shall include a good-faith statement from the complaining party that the material in question violates copyright law.[57]

To balance the rights of copyright owners and users in the digital environment, the statute also provides for the process of counter notification.[58] Under this provision, a user whose material was taken off-line at the request of a copyright owner, has the right to argue (under the penalty of perjury) that the material was removed as a result of mistake or misidentification. Upon receipt of a counter notification, a service provider shall restore access to the allegedly infringing material within 10 to 14 business days unless a copyright owner files an action seeking a restraining court order.[59] The statute provides that a service provider is not liable for disabling access to an allegedly infringing material, even if such material ultimately proves to be non-infringing.[60]

Under OCILLA, copyright owners may request a federal district court to issue a subpoena to a service provider for identification of an alleged infringer.[61] In this case, a service provider is required to disclose to a copyright owner any identifying information it has in its possession. However, a service provider is not expected to contact other systems or networks for information they may have about a potential infringer.[62]

---

55. *See id.* § 512(c)(3).

56. *See id.* § 512(c)(2)(iii, iv).

57. *See id.* § 512(c)(3)(v).

58. *See id.* § 512(g)(3).

59. *See* 17 U.S.C.A. § 512(g)(2)(C) (West Supp. 1999).

60. *See id.* § 512(g)(1).

61. *See id.* § 512(h).

62. *See Report on HR 2281 of the House Comm. on Commerce*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 61 (1998).

OCILLA provides that copyright owners cannot seek monetary relief for activities of service providers that fall within the "safe harbors." However, copyright owners still can seek limited injunctive relief against a service provider.[63] The statute limits injunctive relief to either blocking access to a particular on-line site, or terminating an account of a subscriber who engages in infringing activities.[64] In issuing injunctions, courts shall balance the "magnitude of harm" to a copyright owner against the burden on a service provider and the technical feasibility and efficiency of an injunction. Courts also shall consider the availability of less burdensome and comparably effective means of blocking access to allegedly infringing material.[65]

Finally, the statute provides that nothing in its language shall condone invasion of users' privacy by service providers in the process of monitoring for potential copyright violations.[66]

C. *Legislative History of OCILLA: Evolution of the Knowledge Standard*

1. The White Paper on Intellectual Property and the National Information Infrastructure and 104th Congress

In 1993, the Clinton administration organized a task force on the National Information Infrastructure to "fine tune" the copyright laws to the realities of the digital world. The task force was headed by then-Commissioner of Patents and Trademarks, Bruce Lehman. After numerous public hearings and consultations with 22 federal agencies, the task force came up with a 250-page report, the *White Paper on Intellectual Property and the National Information Infrastructure* (the "White Paper").[67] Addressing the issue of ISPs liability, the report concluded that ISPs should be treated like other distributors under copyright law and that they should be held strictly liable for copyright violations of their users.[68] The report did not recommend any changes

63. *See* 17 U.S.C.A. § 512(j) (West Supp. 1999).

64. *See id.* § 512(j)(1)(A)(iii). Courts are also allowed to order other types of injunctive relief as long as they are "the least burdensome to the service provider among the forms of relief comparably effective for that purpose [restraining infringement of copyrighted material]." *Id.*

65. *See id.* § 512(j)(2).

66. *See id.* § 512(m).

67. Bruce Lehman (ed.), *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights*, Washington, D.C.: Information Infrastructure Task Force, September 1995.

68. "With respect to the allowance of uploading of material by their subscribers, they

to copyright law in regard to ISPs' liability, claiming that existing copyright law could be applied effectively to the Internet.[69]

However, when Senator Orrin Hatch and Representative Carlos Moorehead introduced bills based on the White Paper's recommendations, ISPs and telephone companies immediately criticized them for not addressing the issue of ISP liability.[70] The bills would have extended the copyright owner's exclusive distribution right to include the right of transmission.[71] ISPs argued that, under the proposed legislation, they would be exposed to strict copyright liability each time their users send infringing materials via their networks.[72]

Representative Rick Boucher, a member of both the House Committee on the Judiciary and the House Committee on Commerce, argued during the hearings that Congress should provide ISPs with an incentive to invest in the development of computer networks without fear of litigation. Boucher stressed the importance of balancing the interests of copyright owners on the one hand with the ability of ISPs to thrive on the other.[73]

During the House hearings, representatives of ISPs, such as America Online, Compuserve, and Prodigy, also argued that exposure to strict liability would make them monitor transmissions of subscribers in an attempt to detect infringing content.[74] This could violate First Amendment rights and invade the privacy of Internet users. In addition, they argued, it would be impossible to detect all copyright violations on their networks.[75]

[ISPs] are, in essence, acting as an electronic publisher." *Id.* at 122.

69. According to the report, the Copyright Act of 1976 was "fundamentally adequate and effective" in addressing the new realities of the digital age. *Id.* at 212.

70. H.R. 2441 and S. 1284, 104th Cong. (1995).

71. *Id.* § 2(a).

72. "[T]he main problem ... is a pressure to shift the enforcement responsibility and burden away from copyright owners ... and toward service providers by deeming them violators of the copyright laws essentially, simply by virtue of their presence in the digital infrastructure." *NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong., at 234 (1995) (statement of Stephen Heaton, general counsel for Compuserve, Inc.).

73. *See NII Copyright Protection Act of 1995: Joint Hearing on H.R. 2441 and S. 1284 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary and the Senate Comm. on the Judiciary*, 104th Cong., at 80 (1995).

74. "Service providers must not be required to 'police' or 'monitor' transmissions." *NII Act of 1995: Hearing on S.1284 Before the Senate Comm. on the Judiciary*, 104th Cong., at 38 (1996) (statement of William Burrington, American Online, Inc.).

75. The argument of ISPs was well summarized by Rep. Boucher, who said, "[w]ith transmissions literally numbering in the tens of thousands on a daily basis for a given service,

ISPs also argued that Congress should either immunize them from liability altogether, or hold them responsible for copyright violations of their users only when they have actual knowledge of these violations.[76] This actual knowledge standard could be fulfilled by requiring a copyright owner to notify an ISP of copyright infringements taking place on its network.

Copyright owners, on the other hand, argued that exempting ISPs from strict copyright liability would encourage them to turn a blind eye to on-line violations and would discourage them from cooperating with copyright owners in detecting infringing conduct. For instance, Edward Murphy, president of the National Music Publishers' Association, said: "If an 'actual knowledge' standard advocated by others is allowed to establish a safe haven from the liability for infringements, we fear the creation of an on-line environment in which ignorance is bliss."[77]

Because of the sharp disagreements among copyright owners and ISPs, neither Senate nor House subcommittees took any action on the NII Copyright Protection Act. However, Congress decided to engage the disputing parties in the negotiation process under the supervision of Representative Bob Goodlatte. Goodlatte called for industry negotiations at one of the hearings saying, "[t]his subcommittee [on Courts and Intellectual Property] has a history of preferring that commercial disputes be resolved between the parties rather than through the legislative process, which may favor one interest group over another."[78]

2. WIPO Treaties and 105th Congress

In the period between the 104th and 105th Congresses, the United States became a party to two international copyright treaties negotiated in Geneva at the diplomatic conference held by the World Intellectual Property Organization (WIPO) in December 1996.[79] The

---

that expectation of monitoring is clearly unrealistic." *NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong., at 17 (1995).

76. "[B]ecause providers do not know the contents of the message they are transmitting or distributing on a real-time basis, they are unable to use content as a basis for limiting users' access to their systems unless they have actual knowledge that the material is indeed infringing...." *NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong., at 235 (1995) (statement of Stephen Heaton, general counsel to Compuserve, Inc.).

77. *Id.* at 35.

78. *See id.* at 20.

79. WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty: Message

treaties did not specifically address the issues of ISP liability for copyright violations of their users.[80] However, the delegates to the conference adopted a statement concerning Article 8 of the WIPO Copyright Treaty, according to which "the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention."[81] Thus, WIPO let individual countries establish their own national standards for ISP liability under copyright law.

During the first session of the 105th Congress, several members of Congress introduced bills to implement the WIPO treaties in the United States. Two bills, introduced by Senator John Ashcroft and Representative Howard Coble, addressed the issue of ISP copyright liability.

Senate Bill 1146, the Digital Copyright Clarification and Technology Education Act, sought to shield ISPs from direct, vicarious, and contributory liability when they performed two types of functions: Transmission[82] and temporary storage of material placed by third parties on a system or network.[83] The bill would have covered services such as e-mail, real-time chat,[84] on-line navigational aids,[85] and provision of server space for personal web pages.[86] The bill would have imposed liability on ISPs for copyright violation of their users only if they received a notification from a copyright owner about illegal acts on their networks and failed to remove the allegedly infringing material. The bill was the first to introduce the standard of actual knowledge for ISPs.

However, during the hearings Senator Orrin Hatch, chairman of the Judiciary Committee, stressed that the actual knowledge requirement may not provide an incentive for ISPs to cooperate with

---

from the President of the United States, Apr. 12, 1997, S. TREATY DOC. NO. 105-17 (1997).

80. For a full discussion of the WIPO conference and treaties, see Pamela Samuelson, *The Digital Agenda of the WIPO: The US Agenda at WIPO*, 37 VA. J. INT'L L. 369 (1997). Samuelson writes that there is no international consensus on the issue of whether intermediate copying in computer's memory violates exclusive reproduction rights of copyright owners.

81. *Agreed Statements Concerning the WIPO Copyright Treaty*, Adopted Dec. 20, 1996, WIPO Doc. No. CRNR/DC/96 (1996). The text of the Agreed Statements is available at (visited Mar. 15, 2000) <http://lcweb.loc.gov/copyright/wipo/96dcag.html>.

82. Transmission included three types of services: Transmission of electronic communications (e-mail), provision of real-time services (real-time chat), and supply of information navigational tools (on-line directories and indexes). S. 1146, 105th Cong. § 512(a) (1997).

83. *Id.* § 512(b).

84. *See id.* § 512(a)(2).

85. *Id.* § 512(a)(3).

86. *Id.* § 512(b).

content providers in taking down the pirated sites.[87]

Another bill addressing the issues of ISP liability, House Bill 2180, would have added additional criteria for determining direct and vicarious liability of ISPs, including the knowledge requirement.[88] The knowledge requirement proposed in the bill would have shielded an ISP from copyright liability if it "did not know, and was not aware by notice or other information indicating, that the material was infringing."[89] Representative Howard Coble, sponsor of the bill, explained that this provision introduced an intermediate knowledge standard—something between the actual knowledge and a general standard of negligence.[90] According to Coble, this intermediate knowledge standard was based on the concept of "red flags"—facts, which, even in the absence of notification from a copyright owner, indicate existence of copyright violations.[91]

However, during the hearings held by the House Judiciary Committee, representatives of ISPs and telephone companies criticized this intermediate standard of knowledge as imposing "horrendous liability on carriers, on telephone companies and ISPs."[92] Representative Boucher once again spoke in favor of the actual knowledge requirement and mandatory notice and take-down procedure.[93] However, the Register of Copyrights, Marybeth Peters,

---

87. Senator Hatch stated:

> It seems to me that the content providers make a valid point when they ask what incentives the service providers will have to continue cooperating with them to take down pirated sites. It seems realistic to assume that not all service providers are as ethical or as upright as you folks represented here today ....

The Copyright Infringement Liability of Online and Internet Service Providers: Hearing on S. 1146 Before the Senate Comm. on the Judiciary, 105th Cong., at 41 (1997) (statement of Sen. Orrin Hatch).

88. H.R. 2180, 105th Cong. (1997).

89. *Id.* § 512(a)(F)(i).

90. *The Online Copyright Liability Limitations Act:* Introductory Remarks, 105th Cong., 144 CONG. REC. E1452 (daily ed. July 17, 1997) (statement of Hon. Howard Coble).

91. *Id.*

92. *WIPO Copyright Treaties Implementation Act, and Online Copyright Liability Limitation Act: Hearings on H.R. 2281 and H.R. 2280 Before the House Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary*, 105th Cong., at 82 (1997) (statement of Roy Neel, president of U.S. Telephone Association).

93. Rep. Boucher stated:

> If the content provider knows that an infringement is taking place, the avenue for obtaining relief should be to provide notice and a reasonable opportunity for the OSP to take that information down.... Under the bill as drafted, OSP would be liable for third-party infringement in instances where they have less than actual knowledge of the infringement.... It should be replaced by the actual knowledge standard.

said that such a requirement would violate the provisions of the Berne Convention and the TRIPS agreement[94] against imposition of formalities on copyright owners.[95]

Representative Howard Berman best summarized the gist of the dispute about the knowledge standard for ISPs. Berman suggested that a compromise be found in establishing an intermediate knowledge standard. He stated that: "The answer is somewhere between the conduit, who everybody agrees should not be liable, and . . . something less than actual knowledge."[96]

In February 1997, after several months of negotiations between ISPs and copyright owners, Representative Coble re-introduced the Online Copyright Infringement Liability Limitation Act as House Bill 3209, which replaced his earlier House Bill 2180.[97] The new bill sought to shield ISPs from direct liability for copyright violations occurring in the process of intermediate storage and transmission over their networks.[98] In addition, the bill provided that an ISP should not be liable for monetary damages for contributory or vicarious infringement, when (among other conditions), an ISP "does not know and is not aware of information indicating that the material is infringing."[99] As Coble noted in his introductory remarks, the knowledge requirement in House Bill 3209 was "nearly identical" to that used in House Bill 2180.[100]

Coble explained that "information indicating that the material is infringing" would include "a notice or any other 'red flag'—information of any kind that a reasonable person would rely upon."[101] Such information, he wrote, would include the absence of digital watermarks or other copyright management information. Coble stressed that the bill would not impose on ISPs any affirmative duty to seek out copyright violations on-line.[102]

In his introductory remarks, Coble wrote that he intended to

Id. at 29 (statement of Rep. Boucher).

94. The agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) is a part of the General Agreement on Tariffs and Trade (GATT).

95. *WIPO Copyright Treaties Implementation Act, and Online Copyright Liability Limitation Act: Hearings on H.R. 2281 and H.R. 2280 Before the House Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary*, 105th Cong., at 58 (1997).

96. *Id.* at 187.

97. H.R. 3209, 105th Cong. (1997).

98. *Id.* § 512(a)(1).

99. *Id.* § 512(a)(3)(A).

100. 144 CONG. REC. E160 (daily ed. Feb. 12, 1998) (statement of Hon. Howard Coble).

101. *Id.*

102. *See id.*

codify the court's decision in *RTC v. Netcom*[103] which established liability standards for ISPs.[104] Coble also stressed that the bill intended to overturn the court's holding in *Playboy Enterprises v. Frena*,[105] "inasmuch as that case might apply to service providers, suggesting that such acts could constitute direct infringement."[106]

The debate surrounding the issue of ISP liability culminated on March 31, 1998, with an agreement between copyright owners and ISPs.[107] The next day, the House incorporated this agreement into House bill 2281 (which included House bill 3209).[108] A month later, the Senate adopted the same language in the companion Bill 2037, introduced by Senator Orrin Hatch.[109]

The industry agreement shielded ISPs, under certain conditions, from all types of liability and monetary damages for digital network communications and system caching.[110] It also defined a new standard of knowledge in regard to two other types of functions: Temporary storage of information on networks and information location tools. The new knowledge requirement provided that an ISP shall not be held liable for certain activities if it "does not have actual knowledge that the material or activity is infringing or, in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent."[111] According to the agreement, ISPs that become aware of such facts or circumstances, have an obligation to take down allegedly infringing material—otherwise, they lose protection of the "safe harbors."[112] Both the House and Senate accepted this standard of knowledge and awareness without modifications, and it became effective in October 1998, when President Clinton signed into law the Digital Millennium Copyright

103. 907 F. Supp. 1361 (N.D. Cal. 1995).

104. *See supra* note 100.

105. 839 F. Supp. 1552 (M.D. Fla. 1993).

106. 144 CONG. REC. E160 (daily ed. Feb. 12, 1998) (statement of Hon. Howard Coble). In *Frena*, the Florida district court held a BBS operator liable for illegal acts of his users even in the absence of knowledge on the part of the operator, who took infringing material off-line immediately after notification. *See* 839 F. Supp. 1552 (M.D. Fla. 1993).

107. *Industry Groups Reach Accord on Online Copyright Liability Legislation*, 55 PAT., TRADEMARK & COPYRIGHT J. 557 (1998).

108. Digital Millennium Copyright Act of 1998, H.R. 2281, 105th Cong. (1998), Tit. II.

109. Digital Millennium Copyright Act of 1998, S. 2037, 105th Cong. (1998), Tit. II.

110. *Agreement on Digital Copyright Liability*, 55 PAT., TRADEMARK & COPYRIGHT J. 564 (1998).

111. *Id.* § (c), (d).

112. *Id.*

Act.[113]

In the House Judiciary Committee report issued in May 1998, House members explained that the new knowledge and awareness standard created a so-called "red-flag" test. The report defined a "red flag" as "information of any kind that a reasonable person would rely upon."[114] According to the report, examples of "red flags" would include the absence of digital watermarks or other copyright management information.[115] Members of the House Judiciary Committee stressed that the newly created knowledge requirement differed from existing law, "under which a defendant may be liable for contributory infringement if it knows or *should have known* that material was infringing."[116]

Two months later, the House Committee on Commerce issued its own report on the Digital Millennium Copyright Act.[117] The section of the report explaining the "red flag" test reiterated the key points from the report prepared by the House Judiciary Committee. The members of the House Commerce Committee defined the "red flag" test in the following way: "[W]hether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances."[118] In addition, it explained that the "red flag" test combined two elements—objective and subjective.[119] The report advised that, in determining whether an ISP was aware of a "red flag," courts should look into the "subjective awareness of the service provider of the facts or circumstances in question."[120] However, the report also stated that in deciding whether facts or circumstances constitute a "red flag," courts should apply an objective standard.[121] Members of the House Commerce Committee did not clarify the distinction between the objective and subjective tests that courts should apply in determining whether an ISP was aware of a copyright violation.

---

113. Digital Millennium Copyright Act of 1998, PL 105-304, Tit. II, § 202(c)(i, ii, iii) and (d)(1)(A, B, C) (1998).

114. *WIPO Copyright Treaties Implementation Act and Online Copyright Infringement Liability Limitation: Report on H.R. 2281 of the House Comm. on the Judiciary*, Rept. 105-551, Pt. 1, 105th Cong., at 25 (1998).

115. *See id.*

116. *Id.*

117. Digital Millennium Copyright Act of 1998*: Report on H.R. 2281 of the House Comm. on Commerce*, Rept. 105-551, Pt. 2, 105th Cong. (1998).

118. *Id.* at 53.

119. *See id.*

120. *Id.*

121. *See id.*

The report prepared by the Senate Judiciary Committee in May 1998, described the "red flag" test in terms similar to those used by the House Commerce Committee. Senate members clarified that the new test did not create an affirmative obligation on part of an ISP to monitor its networks or to seek out copyright violations.[122] However, if a provider became aware of a "red flag," it would lose the "safe harbor" protection unless it took steps to remove infringing content off-line.[123]

In October 1998, members of the House and Senate met in a conference committee and prepared a conference report on the Digital Millennium Act.[124] Members of the conference committee stressed that the new liability standard for ISPs was designed to preserve "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[125] The only disagreement between the two houses on the limitation of liability provisions concerned the standards of liability for non-profit educational institutions in their capacity as service providers. The House version of the bill would have relieved institutions from certain types of liability when they passively transmit communications initiated by a student or a faculty member.[126] The Senate version of the bill would have required the Register of Copyrights to consult with representatives of copyright owners and educational institutions and to submit to Congress recommendations regarding the liability of institutions for third-party copyright violations.[127]

In the process of negotiating the bill's provisions, the two houses agreed on a different knowledge standard for educational institutions.[128] Members of Congress made it very difficult to sue institutions for on-line copyright violations committed by their faculty and graduate students. The bill provided that educational institutions

---

122. *See* Digital Millennium Copyright Act of 1998*: Report on S. 2037 of the Senate Comm. on the Judiciary*, Rept. 105-190, 105th Cong. (1998).

123. *See id.* at 44.

124. Digital Millennium Copyright Act of 1998: *Conference Report on H.R. 2281*, Rept. 105-796, 105th Cong. (1998).

125. *Id.* at 72.

126. *See* COMM. ON THE JUDICIARY HOUSE OF REPRESENTATIVES, 105th Cong. 2d Sess., SECTION-BY-SECTION ANALYSIS OF H.R.2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 26, at 28 (Comm. Print Serial No.6 1998).

127. *See* Digital Millennium Copyright Act of 1998: *Report on S. 2037 of the Senate Comm. on the Judiciary*, Rept. 105-190, 105th Cong., at 56 (1998).

128. *See* Digital Millennium Copyright Act of 1998: *Conference Report on H.R. 2281*, Rept. 105-796, 105th Cong., at 74-75 (1998).

would be presumed to know about third-party violations only if infringing materials were a part of the required course list for the class taught at an institution for the past three years; and if the institution received more than two notifications of copyright violations and failed to act on them.[129]

D. Suggestions for Court Interpretation of the New Knowledge Requirement

The new definition of the knowledge standard is at best vague. The phrase, "facts and circumstances, from which copyright infringement is apparent," gives courts the discretion to decide what they consider "apparent" violations of copyright on Internet networks.

For example, when compilers of Internet directories come across a fan site with a large picture of the Star Trek starship, should they consider it an "apparent" copyright infringement and block access to the site? This violation would probably be "apparent" to Viacom and Paramount Pictures, which produce the Star Trek series. However, should an ISP be expected to know a copyright violation, when it sees it?

When the language of the statute is not plain on its face, courts often turn to the statute's legislative history to determine the purposes of its enactment and particular activities targeted by the legislation.[130] The following section argues for narrow judicial construction of the new knowledge and awareness standard set by Congress for ISPs in copyright infringement suits. The key tools of statutory construction are, in the order of their importance: Language, structure, and legislative history of the statute.[131] The argument follows this order by: (a) analyzing the "plain language" of the new knowledge provision; (b) comparing it to other parts of the same statute; and (c) considering the purposes with which Congress enacted the legislation.

1. New Knowledge Standard Should be Construed in Comparison With the Language Rejected or Modified by Congress

The new "knowledge and awareness" standard should be construed in comparison with other language considered and rejected by Congress in the process of drafting the statute. For example,

129. *See* 17 U.S.C.A. § 512(e) (West Supp. 1999).

130. *See* Cass Sunstein, *Interpreting Statutes in the Regulatory State*, 103 HARV. L. REV. 405, 416-17 (1989).

131. *See id.* at 414.

Congress did not endorse the language of House Bills 2180 and 3209 which defined the knowledge requirement as "information indicating that the material is infringing."[132] During the House hearings, witnesses testified that this language is too broad and unspecified and, as a result, could expose ISPs to a "horrendous liability."[133]

In addition, the enacted awareness standard falls short of the actual knowledge requirement introduced in Senate Bill 1146. The latter provided that ISPs should be required to take down certain materials only when they are notified of an alleged violation by a copyright owner.[134] This proposal was rejected because copyright owners were concerned that it would encourage ISPs to turn a blind eye to copyright violations on their networks.[135]

Members of the House and Senate also distinguished the new awareness standard from the knowledge standard applied previously by the courts. In cases of contributory infringement, courts applied the test of constructive knowledge: Whether a person knows or should have known about illegal activities.[136] Thus, the constructive knowledge test involves the element of inference—"a process of reasoning by which a fact or proposition . . . is deduced as a logical consequence from other facts."[137] In other words, the constructive knowledge standard does not necessarily require direct evidence of a copyright violation.

On the contrary, the term "apparent" used in the new statute means "manifest," "open to view," or "plain."[138] Therefore, it can be argued that, unlike the test of constructive knowledge, the requirement to be aware of "apparent" copyright violations does not involve the element of logical deduction or inference by an ISP. Under the new law, to imply knowledge or awareness on the part of a

132. H.R. 2180, § 512(a)(1)(F)(i); H.R. 3209, § 512(a)(3)(A), 105th Cong. (1998).

133. *Hearing on H.R. 2281 and H.R. 2180 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong., at 82 (1997) (statement of Roy Neel).

134. S. 1146, 105th Cong, Tit. I, Sec. 102, § 512(b).

135. "Removing the possibility of liability would eliminate the incentive for Internet access providers to help deter infringements. It would discourage them from working with the creative community to combat on-line piracy. We need cooperation, not immunity." *Hearing on S.1146 Before the Senate Comm. on the Judiciary*, 105th Cong., at 15 (statement of Cary Sherman, general counsel to Recording Industry Association of America).

136. *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Communication Serv., 907 F. Supp. 1361 (N.D. Cal. 1995); Marobie-Fl, Inc. v. National Ass'n of Fire and Equip. Distrib. and Northwest Nexus, Inc., 983 F. Supp. 1167 (N.D. Ill. 1997).

137. BLACK'S LAW DICTIONARY 778 (6th ed. 1990).

138. *Id.* at 96.

service provider, infringement should be "plain" and "manifest" to a reasonable person.

In fact, a congressional committee provided examples of when application of the new awareness standard would be appropriate. The section-by-section analysis of the statute performed by the House Committee on the Judiciary states that copyright violations would be apparent from the use of words such as "pirate," "bootleg," or similar slang terms in the Internet addresses of certain web sites.[139]

The analysis of the statutory language, thus, demonstrates that the new knowledge and awareness standard is less stringent than the standard of actual knowledge. However, it is more difficult to prove than the standard of constructive knowledge, applied previously by the courts. Congress intended the new knowledge standard to be applied only under very specific circumstances, where there could be no reasonable doubt as to the illegal character of the activities.

2. Structural Analysis: Congress Intended Courts to Narrowly Construe the Statutory Provisions that Impose Burdens on ISPs

When the language of the statute leaves doubts about the way a certain provision should be interpreted, courts often turn to the statute's overall structure. It can be argued that the new knowledge and awareness standard calls for narrow interpretation because Congress intended courts to interpret narrowly other provisions of the same statute. Examples of such narrow construction include the knowledge standard for nonprofit educational institutions,[140] the concept of "direct financial benefit" attributable to infringing activities,[141] imposition of injunctions on ISPs,[142] and the requirement that ISPs must release to copyright owners information about their

139. COMM. ON THE JUDICIARY HOUSE OF REPRESENTATIVES, 105th Cong. 2d Sess., SECTION-BY-SECTION ANALYSIS OF H.R.2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 26, at 33 (Comm. Print Serial No.6 1998).

140. The statutes defines the principles of copyright liability for nonprofit educational institutions in section (e). *See* 17 U.S.C.A. § 512(e) (West Supp. 1999).

141. The concept of a financial benefit directly attributable to infringing activities originates in the theory of vicarious liability. According to this theory, a person may be found responsible for illegal acts of others if he or she derives financial benefit from illegal activities and has the right and ability to control them. The new statute incorporates the element of direct financial benefit in sections (c) and (d). *See id.* § 512(c)(1)(B), (d)(2).

142. Title II of the Digital Millennium Copyright Act provides that copyright owners may seek a limited injunctive relief against ISPs. *See id.* § 512(j). An injunction is a court order prohibiting someone from doing certain specified acts. *See* BLACK'S LAW DICTIONARY 784 (6th ed. 1990).

subscribers when issued a subpoena.[143]

During the conference proceedings, members of Congress designed a provision addressing the liability of nonprofit educational institutions, in their capacity as service providers, for copyright violations committed by their faculty and graduate students. The statute provides that an institution would be held liable for third-party violations only a) if the infringing materials were required or recommended for a course taught at a university during the preceding three years, b) if the institution during these three years has received more than two notifications of a copyright violation and failed to act on them.[144]

This provision makes it very hard to sue a nonprofit educational institution for a copyright infringement by one of its employees. First, it takes more than two valid notifications from a copyright owner informing the institution of alleged copyright violations. Second, the course for which infringing materials were used must be taught for at least three years. Third, in the conference report Congress defined "required or recommended" materials very narrowly, as "instructional materials that have been formally and specifically identified in a list of course materials that is provided to all students enrolled in the course for credits."[145] For example, this definition would not include materials distributed by a professor or a graduate student once an academic semester has started, or posted on a class web site without being formally included on a list of required readings.

Therefore, for an institution to become liable for third-party violations, it has to blatantly ignore the facts of copyright infringement identified at least twice, in good faith, by copyright owners.

Another concept that requires a narrow judicial construction is that of "a financial benefit directly attributable to the infringing activity."[146] Some legal scholars interpreted the California federal district court's decision in *Fonovisa Inc. v. Cherry Auction, Inc.*[147] as

143. OCILLA provides that copyright owners can request a federal district court to issue an ISP a subpoena, requesting the release of information identifying an alleged infringer. *See* 17 U.S.C.A. § 512(h) (West Supp. 1999).

144. *See id.* § 512(e).

145. Digital Millennium Copyright Act: *Conference Report on H.R. 2281*, Rept. 105-796, 105th Cong. 2d Sess., at 75 (1998).

146. 17 U.S.C.A. § 512(c)(1)(B), (d)(2) (West Supp. 1999). "Direct financial benefit" is an element of the test for establishing vicarious liability.

147. 76 F.3d 259 (9th Cir. 1996). In *Fonovisa*, the Ninth Circuit Court of Appeals held a

exposing ISPs to vicarious liability for illegal activities of their users, because they derive financial benefit from the monthly subscription fees.[148] In addition, infringing activities arguably may attract new subscribers to ISPs.

Addressing these concerns, the report of the House Committee on Commerce advised courts to take a "common-sense, fact-based" approach to the requirement of direct financial benefit from infringing activities.[149] The report stressed that a "direct benefit" concept would not include one-time set-up fees and flat periodic payment, or fees based on the length of a message. According to the report, courts should apply the concept of direct financial benefit only in the circumstances where, "the value of the service lies in providing access to infringing materials."[150]

Therefore, the concept of a direct financial benefit, as explained by Congress, would apply only to pirate directories which make their revenue by providing access to unauthorized materials on-line. At the same time, the concept of direct financial benefit would not apply to an ISP that has at least some subscribers who engage in legal activities.

Another example of the statute's provision that calls for narrow judicial construction is the disclosure of information about an alleged infringer by a service provider, who received a subpoena.[151] The report of the House Commerce Committee explained that such disclosure should be interpreted as "requiring disclosure of information in the possession of the service provider, rather than obliging the service provider to conduct searches for information that is available from other systems or networks."[152] In other words, Congress instructed courts to construe the disclosure provision narrowly, without imposing additional burdens on ISPs.

The provision establishing standards for injunctions against ISPs is yet another example of the legislative intent to interpret narrowly

---

flea market operator contributorily and vicariously liable for an independent vendor's sale of bootleg recordings. The court decided that the flea market operator reaped financial benefits from admission fees, parking fees, food and other service expenses paid by customers, "who want[ed] to buy the counterfeit recordings at bargain basement prices." *Id.* at 263.

148. *See* Shulman, *supra* note 26.

149. Digital Millennium Copyright Act of 1998: *Report of the House Committee on Commerce on H.R. 2281*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 54 (1998).

150. *Id.*

151. *See* 17 U.S.C.A. § 512(h) (West Supp. 1999).

152. *Report on H.R. 2281 of the House Comm. on Commerce*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 61 (1998).

some of the statute's provisions.[153] The statute instructs courts to consider several criteria before issuing injunctions against ISPs. In particular, courts shall consider if an injunction balances the "magnitude of harm" to a copyright owner against considerations of burden on an ISP, technological feasibility, and effectiveness of injunctions and availability of other, less burdensome and effective means of preventing access to infringing materials.[154] By imposing specific restrictions on issuance of injunctions against ISPs by courts, Congress demonstrated that injunctive relief should be used very sparingly, as the last recourse.

3. The Purpose of the New Statute is to Encourage ISPs to Invest in the Internet Development by Limiting Their Vulnerability to Copyright Litigation

One of the main purposes in limiting ISPs liability for third-party infringements was to encourage economic growth and technological development of the Internet. Members of Congress realized that ISPs should not fear creating new services and continuing to invest in the development of digital networks. For example, the House Committee on Commerce stressed in its report the importance of balancing the interests of copyright owners, Internet providers and Internet users to "foster the continued development of electronic commerce and the growth of the Internet."[155]

Senator Hatch expressed the same idea speaking on the Senate floor before the passage of the conference report, saying "[t]he OSPs [on-line service providers] and ISPs need more certainty in this area in order to attract the substantial investments necessary to continue the expansion and upgrading of the Internet."[156]

One of the ways to encourage activities of ISPs is to limit their exposure to strict liability under copyright law. On numerous occasions, members of the House and Senate stressed that the new statute is designed to clarify provisions of copyright law and to provide greater certainty for service providers as to their duties and rights in the digital environment.[157]

---

153. *See* 17 U.S.C.A. § 512(j)(2) (West Supp. 1999).

154. *See id.*

155. Digital Millennium Copyright Act of 1998: *Report of the House Committee on Commerce on H.R. 2281*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 21 (1998).

156. 144 CONG. REC. S11889 (daily ed. Oct. 22, 1998) (statement of Sen. Hatch).

157. *See* Conference Report: "Title II provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their

The report of the House Committee on Commerce specifically addressed the issue of potential exposure to copyright liability of information location tools including Internet directories such as Yahoo!. The report stressed that further development of navigational tools is "essential to the development of the Internet; without them [information location tools], users would not be able to find the information they need."[158] Members of Congress wrote that on-line catalogers should not be penalized for exercising "human judgment and editorial discretion" by being subject to copyright liability whenever they come across a site that might be infringing.[159] According to the report, liability should not attach to a directory provider for simply seeing, during a brief cataloguing visit, several "well known photographs of a celebrity at a site devoted to that person."[160] The report stated that ISPs cannot be expected to know whether the image is still copyrighted or in the public domain, or whether it is licensed or used under the fair use doctrine.

Members of Congress realized that if the knowledge of copyright infringements is imputed to an on-line cataloguer every time he or she comes across questionable content, ISPs would have little incentive to use man-made on-line directories or would extensively censor on-line speech. For example, the House Commerce Committee report stated: "The knowledge or awareness standard should not be applied in a manner which would create a disincentive to the development of directories which involve human intervention."[161]

Therefore, one of the key purposes in enacting the ISP liability limitation statute was to encourage development of the on-line services by shielding them from extensive litigation.

4. By Limiting ISPs' Liability, Congress Intended to Place Primary Responsibility in Detecting Copyright Violations on Copyright Owners

Members of Congress wanted to make certain that the responsibility of fighting on-line copyright violations would be distributed fairly among copyright owners and ISPs.[162] Many

activities." Rept. 105-796, 105th Cong. 2d Sess., at 72 (1998).

158. *Report of the House Committee on Commerce on H.R. 2281*, Rept. 105-551, Pt. 2, 105th Cong. 2d Sess., at 58 (1998).

159. *Id.*

160. *Id.* at 57-58.

161. *Id.* at 58.

162. *See NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary*, 104th Cong., at

congressional discussions stressed that service and content providers have a common interest in developing the full potential of the Internet, and thus should share responsibility for detecting copyright abuses. For example, the conference report describes the purpose of the liability provisions as preserving "incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[163]

However, Congress decided that it should be the primary responsibility of copyright owners to police the net for potential copyright violations because they are in the best position to make well-informed judgments whether a certain use constitutes a copyright violation. The report of the House Commerce Committee states that ISPs cannot be expected to know whether a certain use is licensed or allowed under the fair use doctrine.[164]

In fact, Congress went to great lengths to make clear that only "obvious" violations would imply "awareness" on the part of an ISP. For instance, the House Judiciary Committee explained that under the new knowledge requirement, an ISP "would not qualify for the safe harbor if it turned a blind eye to 'red flags' of obvious infringement."[165] Examples of "obvious" violations would include pirate directories containing links to big volumes of unauthorized materials, such as copyrighted audio and video clips.[166]

Congress carefully designed the statute to make sure that the key responsibility in resolving copyright disputes lies with copyright owners and Internet users. The statute provides for the notification procedure when a copyright owner lets an ISP know about potential copyright violations on its network.[167] In order to be actionable, a notification must contain a copyright owner's good-faith statement that a violation occurred.

In addition, the statute provides for the procedure of a counter notification, allowing an Internet user to disagree with the copyright

---

19 (1996) (statement of Rep. Sonny Bono).

163. H.R. CONF. REP. NO. 105-796, at 72 (1998).

164. H.R. CONF. REP. NO. 105-551, Pt. 2, at 58 (1998).

165. *See* COMM. ON THE JUDICIARY HOUSE OF REPRESENTATIVES, 105th Cong. 2d Sess., SECTION-BY-SECTION ANALYSIS OF H.R.2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 26, at 33 (Comm. Print Serial No.6 1998).

166. "Location was clearly, at the time the directory provider viewed it, a 'pirate site' of the type described below, where sound recordings, software, movies, or books were available for unauthorized downloading, public performance, or public display." H.R. REP. NO. 105-551, Pt. 2, at 57 (1998).

167. *See* 17 U.S.C.A. § 512(c)(3) (West Supp. 1999).

owner's claims.[168] Both notification and counter notification procedures were designed to make certain that the primary responsibility in resolving difficult issues of copyright law lies with the parties best suited to address them—copyright owners and alleged infringers.

The role of ISPs, on the contrary, is to educate their subscribers by implementing a copyright policy.[169] Such policy would warn Internet users that if they violate copyright laws, ISPs will take down their materials.

II. CONCLUSION

The language, structure, and purpose of the Online Copyright Infringement Liability Limitation Act indicate that Congress recognized the important role ISPs play in the development of the on-line infrastructure and tried to ensure that measures restricting their operation would be used sparingly.

In particular, courts should construe narrowly the new knowledge and awareness standard articulated in OCILLA. Otherwise, ISPs would have an incentive to restrict more on-line speech than necessary to enforce copyright law on the Internet. For example, on-line catalogers should not be expected to detect copyright violation simply by visiting web sites with the posted celebrity photos or images of famous cartoon characters. As long as there is a reasonable element of doubt whether a certain use is licensed or excused under the fair use doctrine, ISPs should not take the material down.

The legislative history of the statute shows that Congress intended the new awareness requirement to apply under very narrow, specific circumstances. For example, when web sites contain words such as "pirate" and "bootleg." The language and structure of the statute also indicate that the primary responsibility in detecting copyright violations on-line lies with copyright owners.

168. *See id.* § 512(g)(3).

169. *See id.* § 512(i)(1)(A).

ESSAY

ARE BUSINESS METHOD PATENTS BAD FOR BUSINESS?

Rochelle Cooper Dreyfuss[†]

TABLE OF CONTENTS

This is an exciting time at which to be involved in intellectual property. When I began teaching, this field was something of a backwater. Around thirty people took my introductory course; only seven went on to study patent law. Indeed, patent law was so esoteric, practitioners were historically among the very few lawyers ethically permitted to advertise their specialty.[1]

In the last decade, however, all of that has changed. Not only are there many more students, what is really interesting as is the level of attention that this field is now receiving from Congress and the courts. Many new rights are being recognized, and old ones are expanding. Trademark holders now enjoy protection that goes well beyond the classic case of passing off. Actionable harms have come to include tarnishment, blurring, and cybersquatting, as well as both post-sale

[†] Professor of Law, NYU School of Law and Director, Engelberg Center on Innovation Law and Policy. This article is based on a speech delivered at Santa Clara University School of Law. I would like to thank the Law School for inviting me and members of the audience for the many interesting ideas they gave me. This work was supported by the Filomen D'Agostino and Max E. Greenberg Research Fund of the N.Y.U. School of Law.

1. *See, e.g.*, MODEL RULES OF PROFESSIONAL CONDUCT Rule 7.4; John A. Payton, Note, *Certification of Specialization: Another Limit on Attorney Advertising Is Peeled Away*, 25 IND. L. REV. 589, 611 (1991).

and initial-interest confusion.[2] According to the Supreme Court's opinion in *Feist Publications, Inc. v. Rural Telephone Service Co.*,[3] fact works are supposed to remain in the public domain. But no matter. Increasingly, they are protectable—through encryption (itself protected by the Digital Millennium Copyright Act[4]), by contract,[5] by the tort of misappropriation,[6] and soon, perhaps, through the Uniform Computer Information Transactions Act[7] and a federal database statute.[8] But the development that has probably caused the most concern is *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*,[9] the Federal Circuit decision recognizing business method patents. Think how the airline industry might now be structured if the first company to offer frequent flyer miles had enjoyed the sole right to award them or how differently mergers and acquisitions would be financed (and how rich Michael Milken might have become) if the use of junk bonds had been protected by a patent. The trend toward expanding protection deserves attention, with the advent of business method patenting deserving the most attention of all.

In many ways, this expansion in rights is not surprising. Information products are now a large part of the economy and for the first time, leading economic indicators reflect their contribution to prosperity. That is, for many years, productivity figures were stagnant, and this was true despite the invention and widespread adoption of the computer, which everyone was sure had to be increasing productivity. There was much headscratching about why the numbers weren't rising—whether social dislocations caused by technology outweigh benefits; whether economists were unable properly to evaluate the service economy or to grapple with units of production that, over time, become more complex rather than cheaper.[10] Recently, however, the productivity figures have started to

2. *See* 15 U.S.C.A. § 1125(a)-(d) (West 1998 & Supp. 2000); Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999); Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 799 F.2d 867 (2d Cir. 1986).

3. 499 U.S. 340, 350-51 (1991).

4. *See* 17 U.S.C.A. § 1202 (West Supp. 1999).

5. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).

6. *See, e.g.*, Board of Trade v. Dow Jones & Co., 98 Ill.2d 109 (1983).

7. *See* UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (1999).

8. *See* H.R. Rep. No. 106-349, at 2, 9 (1999) (accompanying H.R. 354 to provide protection for "certain collections of information").

9. 149 F.3d 1368 (Fed. Cir. 1998), *cert. denied*, 119 S. Ct. 851 (1999).

10. *See, e.g.*, Zvi Griliches, *Productivity, R&D, and the Data Constraint*, AM. ECON. REV., Mar. 1994, at 1.

move,[11] allowing Congress and the American people to appreciate the value of intellectual work, and to perceive the benefits of supporting the creative community with intellectual property rights. Even the gap between the introduction of computers and rising productivity makes that point. Why, in the end, *did* it take so long for productivity to increase? The answer, perhaps, is that inventing a new technology is not enough. Also required is a killer application, an application that inspires people to learn how to use the new development. Even after that, routine business applications are needed to give those who learned the new technology, opportunities to exploit their knowledge in ways that are fruitful for the economy. And that is where business method patents would seem to enter the picture, the argument being that not only does society need patents to motivate technological advances, it also needs them to motivate the business restructuring required to take full advantage of new developments. Indeed, the case for business method patents may seem so obvious, nonpatent lawyers may find it surprising to learn they have not always been available. But such is the case, at least officially: it was only two years ago that *State Street* gave judicial recognition to business method patents.

As noted, patent protection for business methods certainly appears to be a good idea. But is it? Are there problems with this sudden change in the law? Is *State Street* really going to lead us to Easy Street? This paper examines the decision, describes the layers of difficulties it presents, and then asks what, as a society, we should do about this part of the trend toward ever stronger intellectual property rights.

I. STATE STREET

State Street involves a patent entitled "Data Processing System for Hub and Spoke Financial Services Configuration."[12] The invention keeps track of individual mutual fund investments ("spokes") which have been pooled into a single portfolio (a "hub"). Essentially, what the system does is generate numbers that represent (among other things) each spoke's share of profits, numbers that are needed to comply with a set of Internal Revenue Service (IRS)

11. *See, e.g.*, Louis Uchitelle, *U.S. Productivity Rose at 5% Rate in 2nd Half of '99*, N.Y. TIMES, Feb. 9, 2000, at A1.

12. U.S. Pat. No. 5,193,056.

Regulations.[13]

The patent was attacked on two interrelated grounds. First, there was the "software" problem. Courts have always had trouble with process patents because they are afraid that the claims in these patents are really drawn to principles of nature, which must remain in a domain where they can be used by all. Traditionally, the Supreme Court's solution to the problem of differentiating processes that are principles from processes that are patentable applications, has been to restrict patents to those processes that effect transformations in the physical world—for example, sifted flour;[14] separated glycerine;[15] or cured rubber.[16] But since the invention in *State Street* produced, basically, numbers, the argument was made that the invention was more akin to $E = mc^2$ or the pythagorean theorem than to a patentable invention.[17]

For its part, the Court of Appeals for the Federal Circuit had developed a more sophisticated way to distinguish algorithms found in software from abstract principles. Under its *Freeman-Walter-Abele* analysis, patents were upheld when the claims were drawn to a specific machine or the algorithm was made a part of a larger physical process or method.[18] In *State Street*, the patentee had, in fact, tried to fit within the latter category by claiming that the algorithm at issue was part of a method of doing business. That approach was, however, susceptible to a second challenge, one based on a long line of (mainly lower) court opinions holding that business methods are too abstract to be patented.[19]

Siding with the unauthorized user, the District Court accepted both of these arguments. However, matters went surprisingly differently on appeal. The case was assigned to Judge Giles Rich.

---

13. *See* I.R.C. 701-706 (West 1998 & Supp. 1999); Treas. Reg. § 1.704-1 to 1.704-4 (as amended in 1997); *see also* Leo I. Raskind, *The Bad Business of Business Method Patents*, 10 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 61, 86 (1999).

14. *See* Cochrane v. Deener, 94 U.S. 139 (1877).

15. *See* Tilghman v. Proctor, 102 U.S. 707 (1880).

16. *See* Diamond v. Diehr, 450 U.S. 175 (1981).

17. 927 F. Supp. 502, 516 (D. Mass. 1996) (Saris, J.), *rev'd*, 149 F.3d 1368 (Fed. Cir. 1998).

18. *See In re* Alappat, 33 F.3d 1526 (Fed. Cir. 1994); *In re* Abele, 684 F.2d 902 (C.C.P.A. 1982); *In re* Walter, 618 F.2d 758 (C.C.P.A. 1980); *In re* Freeman, 573 F.2d 1237 (C.C.P.A. 1978); *see also* Arrhythmia Research Tech., Inc. v. Corazonix Corp., 958 F.2d 1053, 1060-61 (Fed. Cir. 1992).

19. *See, e.g.*, Loew's Drive-In Theatres, Inc. v. Park-In Theatres, Inc., 174 F.2d 547, 552 (1st Cir. 1949), *cert denied*, 338 U.S. 822 (1949); Hotel Sec. Checking Co. v. Lorraine Co., 160 F. 467, 469 (2d Cir. 1908).

An ex-patent attorney, Judge Rich was also reputed to have been the principal drafter of the current (1952) Patent Act, and by the time he wrote this opinion, rumored to be the longest-sitting federal judge.[20] This was one of his last opinions, and he apparently decided to go out with a splash. First, he repudiated *Freeman-Walter-Abele* on the way to distinguish applied software from principles. Instead, he laid down a rather simple test, holding patentable any transformation of data that produces "a useful, concrete, and tangible result."[21] Next, Judge Rich ran through that case law on business methods to show that the statements on their nonpatentability were pure dictum.[22] He concluded: "Since the 1952 Patent Act, business methods have been, and should have been, subject to the same legal requirements for patentability as applied to any other process or method."[23]

State Street thus makes two changes in the law. It does away with special rules for determining when software is patentable subject matter and it brings business methods into the ambit of protection. In the latter connection, it is important to note that *State Street* apparently makes patentable all business methods: although the case itself was about a computer-implemented business method, the language of the opinion is extremely broad.

II. IMPLICATIONS OF BUSINESS METHOD PATENTING

This brings us to my questions. Clearly, society needs people to develop new business methods—that is the import of the story about the productivity numbers. But is it right to encourage them to do this through patent law? I see two difficulties with moving in that direction: one concerns the quality of the business patents that are issuing; the other, the wisdom of recognizing exclusivity in competitive processes.

A. Quality

The first problem is one that concerns many observers of the

20. *See* Richard A. Oppel, Jr., *Giles S. Rich, Oldest Active Federal Judge, Dies at 95*, N.Y. TIMES, June 12. 1999, at A13; Jon Thurber, Obituaries, *Judge Giles Rich; Patent Law Authority*, L.A. TIMES, June 14, 1999, at A22. Judge Rich was first appointed to the bench in 1956 and remained on active status until the time of his death 43 years later.

21. 149 F.3d at 1373.

22. *See id.* at 1375-77. Professor John Thomas recently discovered that Judge Rich had relied on this "dictum" himself. *See* Giles S. Rich, *Principles of Patentability*, 28 GEO. WASH. L. REV. 393, 393-94 (1960).

23. 149 F.3d at 1375.

patent system. It is the frequency with which the Patent Office issues patents on shockingly mundane business inventions. The most notorious example is probably Jay Walker's Priceline patent, which inspired the following comment from a reader of Forbes Magazine: "Cool! Jay Walker has apparently patented the 'business method' known as a Dutch auction—a method by which the U.S. Treasury sells hundreds of billions of dollars' worth of securities each year."[24] And there are many other examples as well. Professor John Thomas at George Washington cites a method for running a remodeling business that comprises cataloging ideas, presenting the ideas to a client, allowing the client to select an idea, and then showing the client a picture of his or her selection.[25] My personal favorite is in the field of architecture. It is a method for eliminating hallways through the process of placing the staircases on the outside of buildings.[26]

Admittedly, what is particularly bad about these patents is that the methods they protect were well known before the applicant came along. For example, anyone familiar with Bergin Hall at Santa Clara University School of Law knows all about the concept of the outside staircase. On that issue, it must be said that Judge Rich never intended for known business methods to be patented. Indeed, he stressed—cautioned—that business methods must meet the other legal requirements for patentability, requirements that include novelty (the method must be new[27]) and nonobviousness (the method must be more inventive than would be expected of an ordinary business person[28]).

But even so, there are problems. Denying patents on known methods is not so easy to do. One problem is conceptual. The standard of novelty and inventiveness are not absolute; they receive coloration from the field at issue in the patent. For example, in chemistry, where basic structures, syntheses, and theory are well known, a fairly low standard of inventiveness is needed if patents are to be available at all. And, in fact, courts have developed a series of subtests that produce exactly the right kind of standard.[29] The same

24. Byron L. Winn, Readers Say, FORBES, May 31, 1999, at 18. Of course, whether Uncle Sam is infringing depends on the scope of protection afforded.

25. *See* John R. Thomas, *The Patenting of the Liberal Professions*, 40 B.C. L. REV. 1139, 1161-62 (1999) (citing U.S. Patent No. 5,668,736).

26. *See* U.S. Patent No. 5,761,857 ("Lot configuration and building position and method for residential housing").

27. *See* 35 U.S.C. § 102 (1994).

28. *See id.* § 103.

29. *See, e.g., In re* Dillon, 919 F.2d 688 (Fed. Cir. 1990) (tracing the history of chemical

can be said about business methods: now that the Federal Circuit has decided they should be considered patentable, the standards will be adjusted to make sure that these patents are generally granted.

Indeed, *Wang Laboratories, Inc. v. America Online, Inc.*,[30] a recent case on infringement, is suggestive on this issue. The question there was patent scope, and the court took a very narrow view of what any particular business methodology teaches. Thus, the case found patent-significant distinctions between two "favorite places" or "bookmark" features, one using bit mapping protocols and the other using a character-based system. Since there is a close connection between scope for purposes of anticipation and scope for infringement,[31] this narrow reading of the claim may foreshadow how prior art will be used in novelty determinations as well. If so, it will take a great deal of prior art to convince a court that a particular method of doing business is obvious or anticipated.

A second reason to be wary of relying solely on novelty and nonobviousness to protect against mundane patents is practical. Consider the observation of Greg Aharonian of Patent-News that the number of non-patent references cited is often very low.[32] In fact, his finding is not very surprising: there are systematic reasons why this should be the case. First, because business methods have not been patented in the past, there is very little patent-related prior art readily at hand to the examiner corps. More important, because knowledge about business methods resides mainly in the practices and policies of the firms that use them, even common methods may not be documented in the sorts of materials that examiners can efficiently consult. Unless these difficulties are taken care of—and it is hard to see how the latter can ever be dealt with effectively—invalid patents will inevitably issue.

Finally, there is a subjective element to patent decisions that needs to be considered. It can be seen in three cases the Supreme Court decided on the same day: *Graham v. John Deere Co.* and *Calmar v. Cook*,[33] were about about a plow and a spray can,

---

nonobviousness); *see also* ROBERT P. MERGES, PATENT LAW AND POLICY 589-90 (2d ed. 1997).

30. 197 F.3d 1377 (Fed. Cir. 1999).

31. *See, e.g.*, Miller v. Eagle Mfg. Co., 151 U.S. 186, 203 (1894). The connection is encapsulated in the familiar saying: "that which infringes if later, anticipates if earlier." *Id.*

32. Gregory Aharonian, Internet Patent News Service, June 23, 1999, *available at* <http://www.bustpatents.com/ipns.htm> (on file with author).

33. 383 U.S. 1 (1966) (consolidated in *Graham v. John Deere*).

respectively, and *United States v. Adams*,[34] was about a battery. The first two patents were invalidated on obviousness grounds, but the third was upheld. It is not easy to distinguish the cases, and many suspect that the different outcomes had more to do with the justices' familiarity with the fields of the invention than with the inventiveness of the advances at issue in the cases. Thus, the plow and the spray can involved mechanicals—hinges, gaskets, ribs, and such. Because judges deal with (or think they should be able to deal with) such devices in their ordinary lives, they may have found it difficult to imagine that a particular arrangement of these familiar objects could be inventive enough to merit protection. But working with electricity can be dangerous; most people stay as far away from it as possible. Free to admit that they lacked intimate knowledge of batteries, the justices were also free to find the invention at issue in *Adams* nonobvious. The general lesson here is this. What judges don't understand, they think is patentable—there is a kind of "gee wiz" factor that is hard to overcome. In contrast, what judges do understand (or think they should pretend they understand), appears obvious—an "I could have done that" view takes hold instead. That is important in this context because it is rather probable that judges do not understand (or bother to pretend they understand) the Internet or software. Thus, we can certainly expect fairly widespread validation of at least certain classes of business method patents.

Of course, one could dismiss the problem of invalid patents as ephemeral—if a patent covers a business method that is really important, it will be challenged and invalidated. But while the potential for successful challenge is certainly real, it is not clear that it is an adequate solution. After all, patents have *in terrorem* effects: no one wants to invest in a business that cannot succeed without first winning a lawsuit. Moreover, much can happen during the transition period between allowance and invalidation. For example, many industries experience shake outs. These have the beneficial effect of culling out those firms that are the least competent. But to some extent, business method patents protect businesses from competition. Thus, they can function in a way that preserves inefficiencies in the marketplace.

In some fields, there is another, more enduring, problem. Take law and medicine: substantial relationships are built (lawyer and client, doctor and patient). Once loyalty develops, whatever business method drew the client to the provider becomes irrelevant; even if the

34. 383 U.S. 39 (1966).

patent on the method is invalidated, the client will stay put. Of course, concepts like "loyalty" and "relationships" are somewhat retro and passe. Now we talk about "stickiness." But this is just a vocabulary shift. As with loyalty, once a sticky method takes hold, invalidation of the patent on that method will make no difference.

This is an important point, so let us examine it with some illustrations. One way to produce a sticky business method is lock in. Consider, for example, Amazon.com's patented one-click technology, which has been enforced against BarnesandNoble.com.[35] One click is very nice for shoppers because once they have inputted various bits of shipping and billing information, they can check out quickly on subsequent visits. Accordingly, if Amazon has the exclusive right to one-click, we can expect that many customers will patronize its site. What happens if the patent is eventually invalidated—will there then be effective competition? Probably not because once a book buyer has entered information at Amazon, there is no reason to go elsewhere, particularly now that Amazon has the capacity to further analyze the information and offer its patrons useful suggestions about future purchases. Buyers who rely on such services will not care if the patent is invalidated, and rival sites are permitted to utilize one-click: once locked in to Amazon, shoppers will not likely visit a site that is less informative and requires more work.

Another way to make customers stick is with network effects. An example of a network effect is AOL's instant messenger.[36] A user's ability to exchange email in real time is useful only when the people the user wishes to reach are also on the same system. As a result, the value of the system as a whole depends directly on its size. I do not know whether AOL has protected its system with a patent, but if it has, then instant messanger is a good example of the problem with relying on invalidation. The reason is this: if there were such a patent, it would be extremely significant because it would force everyone interested in instant messanger to sign up with AOL. But once a large (and valuable) network is created, invalidation will not matter at all. True, rivals would appear, but because they would necessarily start small, they would not be able to deliver the same

35. *See* Amazon.com, Inc. v. Barnesandnoble.com, Inc., 73 F. Supp. 2d 1228 (W.D. Wash. 1999).

36. *See* Saul Hansell, *In Cyberspace, Rivals Skirmish Over Messaging*, N.Y. TIMES, July 24, 1999, at A1 (describing America Online's use of its copyrights and trademarks to reserve its instant messaging service to its own network of subscribers); Leslie Helm, *AOL Aligns with Apple in Instant Messaging Venture*, L.A. TIMES, July 30, 1999, at C3.

value to their customers. The bottom line is thus a terrible transition problem: patents do not need to be in force for long to exert a substantial effect on competition.

Now, it must be admitted that Congress has already noticed that there is a problem here, that examining business methods for novelty and nonobviousness is going to be difficult, and that invalid patents can be problematic. It has even done something to fix the situation. Soon after *State Street*, it enacted the "first inventor" defense (also called a prior user right). Under this provision, there is a defense to infringement in favor of any person who: "acting in good faith, actually reduced the subject matter [of a business method patent] to practice at least one year before the effective filing date of such patent, and commercially used the subject matter before the effective filing date of such patent."[37]

Unfortunately, however, this fix is not enough. It is very limited: in order to prevent the first inventor from competing away all patent profits, the defense can be asserted only by the party who established the defense and it can only be used with respect to the specific subject matter claimed.[38] Furthermore, it can create effective competition only when there is someone who was positioned, before the application was filed, to enter the patentee's business. Most important, recognition of this defense could have perverse effects in future litigation. By creating this defense, Congress may be viewed as having implicitly endorsed business method patenting.[39] Further, the first inventor defense may actually reduce the extent to which other unpublicized inventions will be regarded as prior art in the future.[40]

---

37. 35 U.S.C.A. § 273(b)(1) (West Supp. 2000).

38. *See id* § 273(b)(6) & (b)(3)(C).

39. *Cf.* Oddzon Prods., Inc. v. Just Toys, Inc., 122 F.2d 1396 (Fed. Cir. 1997) (holding that art under 35 U.S.C. § 102(f) can be combined with other art to find an invention nonobvious on the basis that Congress amended § 103 to address the narrow problem of §§ 102(f) and 103 rejections in the context of large-firm research. In so doing, the court ignored the fact that Congress had never, in fact, considered the broader question of whether § 102(f) should *ever* be used for § 103 purposes.).

40. This theory is somewhat controversial and complicated. Section 102(g) refers to inventions "made in this country by another who has not abandoned, suppressed or concealed it." 35 U.S.C. § 102(g) (1994). Although the section is mainly read as limiting the field of who can claim priority, it has been used to protect the reliance interests of those who commercialized inventions without publicizing them. *See, e.g.*, Dunlop Holdings, Ltd. v. Ram Golf Corp., 524 F.2d 33 (7th Cir. 1975); *In re* Bass, 474 F.2d 1276 (C.C.P.A. 1973); Pierre Jean Hubert, *The Prior User Right of H.R. 400: a Careful Balancing of Competing Interests*, 14 SANTA CLARA COMPUTER & HIGH TECH. L.J. 189, 193 (1998). Since the first inventor defense will now be available to protect such users in the case of business methods, see H.R. Rep. No. 106-287, at

There are a few other, and potentially more salutary, developments on the horizon. First, there is building sentiment to improve the performance of the Patent and Trademark Office. For example, Robert Merges recently published an article suggesting better pay and training for examiners; an end to the system of awarding examiners bonuses for final dispositions (which tend to strongly favor allowances, which are not appealed, over disallowances, which are); substantial revision of the reexamination system; and external review of performance.[41] Second, courts may become better at assessing novelty and nonobviousness. Encouraging in this regard is *AT&T Corp. v. Excel Communications, Inc.*,[42] which concerned a telephone billing method. In the first incarnation of that case, the Federal Circuit held the business method patentable subject matter. However, in a later phase, the patent was invalidated as obvious in light of MCI's Friends and Family Program. Third, there is the potential of e-mail and the Internet. We saw their tendency to exacerbate the problems of invalid patents through lock-in and network effects, but they could also be a part of the solution to the problem of bad patents. Thus, for example, the World Wide Web Consortium (W3C) advertised successfully on its web site for art that it later used to defeat a patent on a privacy protection protocol that it was using.[43] Fourth, Leo Raskind has argued that the misuse defense, somewhat moribund in recent years, may enjoy a revival. If, for instance, it were to turn out that the invention in *State Street* is the only efficent way to run the IRS calculations on which it is based, then the patent may be valid, but any failure to license it broadly and on reasonable terms could be regarded as misuse.[44] Finally, there is an aspect of the *Wang* case on "favorite places" technology that is also very hopeful. As we saw, that case involved a valid patent, but the court construed it quite narrowly. If business method claims are similarly limited to specific implementations, they will be much less

---

44-49 (1999), courts may reason that § 102(g) art should not generally be construed as patent-defeating.

41. *See* Robert P. Merges, *As Many as Six Impossible Patents Before Breakfast: Property Rights for Business Concepts and Patent System Reform*, 14 BERKELEY TECH. L.J. 577 (1999).

42. 172 F.3d 1352 (Fed. Cir. 1999).

43. *See* World Wide Web Consortium, *P3P and the Intermind patent* (visited Mar. 27, 2000) <http://www.w3.org/1999/04/P3P-PatentBackground.html>. The ad read as follows: "WANTED: When did you first see a technology like this? ... W3C is looking for information concerning any systems that predate the Intermind patent...." *Id.*

44. *See* Raskind, *supra* note 13. Patents cannot be enforced until misuse is purged. *See* DONALD S. CHISUM, CHISUM ON PATENTS § 19.04[4] (1998).

problematic.

But despite these hopeful signs, I remain concerned about quality. As noted earlier, no one goes out to buy a lawsuit; patents, even invalid patents, exert an influence on the market. Furthermore, as the Federal Circuit strengthens the presumption of validity, these patents become increasingly difficult to challenge.[45]

B. Wisdom

Invalid patents are not, however, my main concern. My real problem with this trend is more controversial: I even question the value of valid business method patents. I believe that they adversely affect innovation, and worse, the economy. These patents are not associated with the benefits that, as a constitutional matter, justify the recognition of private property. And the economic costs they impose can be astounding. Let me take these points one at a time.

As I noted at the outset, business methods are not the only example of newly created or expanded intellectual property rights. There is also database protection, dilution, blurring, cybersquatting, and misappropriation. A strange aspect to many of these expansions is that they occur without any specific thought given to the need for protection. Once a creative product (a mark, a celebrity image, a business method) is recognized as having value, it is assumed that someone has a right to capture that value. Measured against the background of property rights propagation generally, this is a rather novel approach. In the world of tangibles, rights are recognized only when there is a public (not just a private) benefit to be gained: to avoid the tragedy of the commons—to prevent overfishing or overgrazing; to encourage pollution control, resource management, and conservation.[46] Otherwise, the trend in property law has been towards the commons—to creating parks, clean waterways, playgrounds, zoos, and such. In intellectual property law, similar attention was once paid to the question of justifications. The framers of the Constitution, for example, rejected "just deserts" and other

45. *See* 35 U.S.C.A. § 282 (West 1984 & Supp. 1998); Medtronic Inc. v. Intermedics, Inc., 799 F.2d 734, 741 (Fed. Cir. 1986) ("35 U.S.C. § 282 creates a presumption that a patent is valid and imposes the burden of proving invalidity on the challenger by 'clear and convincing evidence.' That burden is permanent and does not change."); *see also* Dickinson v. Zurko, 527 U.S. 150 (1999) (requiring the Federal Circuit to review appeals of PTO decisions on a deferential basis).

46. *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1244 (1968); H. Scott Gordon, *The Economic Theory of a Common-Property Resource: The Fishery*, 62 J. POL. ECON. 124, 134 (1954) (giving an earlier version of the theory of the tragedy of the commons).

moral claims in favor of pure utilitarian approaches. Thus, intellectual property rights generally are basically viewed as solutions to the free rider problem; patents are also valued because they encourage disclosure.[47]

But neither the free-rider nor the disclosure rationale justifies business method patents. Businesses are largely practiced in public. Accordingly, there is little need to especially encourage disclosure. Business methods are also hard to free ride on. They depend in strong ways on the social structure within the firms utilizing them—on compensation schemes, lines of reporting, supervising policies, and other business factors. Moreover, as we saw, sticky business methods are their own reward. With lock in, network effects, and even good old fashioned loyalty, lead time (the first mover advantage) goes a long way to assuring returns adequate to recoup costs and earn substantial profit. In sum, while business innovations are certainly desirable, it is not clear that business method patents are needed to spur people to create them.

On the costs side, matters are even more unfavorable for business method patents. All patents impose social costs. Patented products are more expensive; quantity and quality are less than they would be in a competitive market. Furthermore, there is deadweight loss created as those who would buy the product at the competitive price forgo purchase at the higher patent price. There is also an offsets problem. Because knowledge is cumulative, any rise in the price of using existing intellectual products also increases the cost of innovating future products. Without free and unfettered ability to—in Sir Isaac Newton's words—stand on the shoulders of giants,[48] innovators are not able to push the frontiers of science forward. Spillover benefits are likewise reduced, for the private right to control a new technology can be used to prevent others from applying that technology in ways the rights holder did not consider.

Of course, some patents impose more of these costs than do others. To determine how high costs would run for any particular patent, it is useful to conceptualize knowledge as a pyramid: the big ideas are on top; specific applications are at the bottom. Specific applications are largely dead ends. Private ownership of these

47. *See, e.g.*, Rochelle Cooper Dreyfuss, *Intellectual Property Law*, *in* FUNDAMENTALS OF AMERICAN LAW 507 (Alan B. Morrison, ed. 1996); Edmund Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265 (1977).

48. *See* ROBERT K. MERTON, ON THE SHOULDERS OF GIANTS 31 (1965) (quoting a letter by Sir Isaac Newton).

applications does not entail high social cost because others will never need these inventions as a basis for their own inventiveness. But as one moves up the pyramid, the costs associated with privatization increase. As a result, the big inventions at the top—inventions denominated as ideas or principles—are not considered patentable. They must remain in the public domain because they have instrumental significance. Society needs them to generate other specific applications, and also to open new technological opportunities. The issue, then, is to locate business methods on this pyramid. In fact, they are towards the top. Partly that is so for the familiar reasons just discussed: they are instrumental in the traditional sense, as the basis for further inventiveness. But they are important in another, somewhat different sense as well: they are instrumental to the economy.

To see this, it is helpful to shift gears and to consider a somewhat related issue: should sports moves be patentable? What, for example, if Candy Cummings had patented the curve ball or Dick Fosbury, his high jump "flop?" Would sporting events be as popular? It seems unlikely. After all, sporting events are interesting because they pit humans against one another to determine whose abilities are superior. For that competition to be true, participants need to compete—literally—on a level playing field. Allowing one athlete to use a move that is denied to others would destroy the essence of the event.[49] The same can be said of business methods: winning and losing is supposed to depend on execution, not on exclusive rights to the moves that need to be executed. We want the best book store to dominate the market, not the store that makes it easiest to check out. Or, just as sporting events identify the best athlete and team, market competition is what this society relies on to determine the best use for particular resources. If that mechanism is distorted, then Adam Smith's unseen hand is crippled.

Now, in sports, the problem of patented moves is somewhat reduced because competitions have organizers (for instance, baseball has a commissioner). These organizers can easily ban the use of moves (or products) that are not made available to all. But no one is positioned to do that with respect to business methods: Bud Selig is far more likely to bring John Rocker into line than Joel Klein is to tame Bill Gates.

The bottom line is this. The costs of business method patents are

49. *See generally* Jeffrey A. Smith, Comment, *It's Your Move–No It's Not! The Application of Patent Law to Sports Moves*, 70 U. COLO. L. REV. 1051 (1999).

very high. The benefits, at least the traditional benefits, are low. The ratio is terrible. The case for patents on business methods is simply not there, at least not in general. Indeed, it is almost unnecessary to say this here, at Santa Clara University School of Law in Silicon Valley, where the free flow of information among firms may well have had a great deal to do with economic success.[50] *State Street* now provides the opportunity to tie up such knowledge for the future, to privatize it, and prevent it from leaking out to all users. The firms of this Valley should be the ones most cognizant of the danger this poses to innovation.

III. WHERE TO GO FROM HERE

Given the problem of business method patents, a strong argument can be made that *State Street* should be reversed, either judicially or legislatively. However, these remarks have been coached in general terms; it is not implausible that there are specific areas where business method patents achieve socially useful results. John Thomas, for example, has suggested that method patents should be confined to what he calls the technological arts: production methods rather than lawyering methods; physical, not medical treatments; industrial as opposed to business applications. Thomas bases this suggestion on the Constitution's reference to the "useful arts,"[51] which, he claims, is the 18th Century's word for what we in the 21st Century call "technology."[52]

That would be one cut at the problem, but I am not convinced it is the right one. I do not know what the drafters of the Constitution meant by "useful arts." In addition, it isn't clear to me that the word "technology" is unambiguous enough to create a clear judicial line. Most important, I don't understand why that particular divide would distinguish between fields where patents make sense and fields where they do not. To me, the better way to define the scope of patent protection is by sticking with the question of rationales, by asking where a patent incentive is actually required to promote investment in innovation.

As to that, let us step back to the *State Street* decision one more

50. *See* Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575 (1999).

51. *See* U.S. CONST. art. I, § 8, cl. 2.

52. *See* Thomas, *supra* note 25, at 1164.

time. As we saw, the first part of Judge Rich's opinion made patent protection for software easier to obtain. At one time, I might have had many of the objections to software patenting that I've already voiced with regard to privatizing business knowledge. For instance, it would have slowed progress in this Valley. But at this point in time, the software industry is mature; new developments are hard-fought—increasingly expensive to create, yet they remain cheap to copy. Given that secrecy is also sometimes a real option with software developments, I think we can assume that the first part of the *State Street* decision is good law. If so, then perhaps those business methods that partake of the "software rationale" should also be candidates for protection. That is, I could easily imagine denying protection to the likes of frequent flyer miles, junk bonds, curve balls, and Fosdick flops. But we saw that getting the productivity numbers up after the introduction of computers required both killer and routine applications; encouraging these applications with patents may make some sense. Note, however, that the business method patents that would be allowed under this rationale would be highly limited. *Only* applications—new and nonobvious computer-implementations—would merit protection. In essence, these patents would run to the software, not to the business model that the software implements.

Such an approach has much to recommend it. First, as a theoretical matter, it would achieve congruence with the way that intellectual property law has always treated principles. As we saw, both patent law and copyright distinguish between principles and instantiations of those principles (expressions or applications). An instantiation can be privately owned, but the abstraction must go into the public domain.[53] Under the move suggested here, business models would be dealt with similarly. The abstract model would remain free for all to utilize. However, specific implementations of the model would be considered the subject matter of patent law.

Second, this approach would eliminate the specter of patents in areas that do not need the special incentives of exclusive rights regimes. Junk bonds, for example, are good examples of inventions that generate their own rewards. They do not need patent protection and would not merit it under this system because they do not require software implementation.

Third, this approach would focus the courts on the inventiveness of the software: any sort of "gee wiz" factor deriving from using banal real world business models on the Internet would be eliminated.

53. *See* discussion *supra*.

That in itself would be a substantial accomplishment. As we saw in the quote from Forbes,[54] what strikes many observers as wrong about business method patenting is that to can be used to protect processes whose only inventive features involve the transfer of a well known business model, such as the Dutch auction, to cyberspace.[55] Under the approach suggested here, Internet utilization of real world models might still be patentable, but now only when the translation actually required inventiveness, that is, the creation of nonobvious implementing technology.

Most important, this approach would yield patents of rather narrow scope. The protection would run only against the specific implementation disclosed in the patent; anyone who could implement the business with new software, or utilize it without a computer, would know that such use would escape infringement. Thus, it would be clear to all that the United States could continue to use its method for selling treasury bills even if Walker's Priceline patent is valid. And since other online businesses could imitate the patented business method (Priceline's auction or Amazon.com's one-click) with different software, the distortive impact of these patents on market competition would be minimized.

In the final analysis, there is an irony in *State Street.* The main reason for the increase in business method applications was because *Freeman-Walter-Abele* made patent eligibility for software turn on placing the program into the context of a process. Now that the subject-matter requirement can be met by generating numbers that produce useful, concrete, and tangible results, there is no longer a need for what was, quite frankly, always a bit of a dodge. As we saw, business method patents make little sense from an economic perspective; if they are not even needed to create legal fictions, why recognize them at all?

---

54. *See* Winn, *supra* note 24 and accompanying text.

55. Other examples include two of Amazon.com's best known patents: the patent on one-click basically covers the concept (particularly well known in bars) of asking the seller to put a particular purchase "on my tab." Amazon also has a patent on its affiliates program, which allows web sites to refer customers to Amazon in exchange for a fee. *See Amazon.com Patent Covers Fee Program On Customer Referral,* WALL ST. J., Feb. 28, 2000, at B8; Mo Krochmal & Jason Coombs, *Amazon Associates Plan Wins Patent Protection* (Feb. 25, 2000) <http://www.techweb.com/wire/story/TWB20000225S0013>. That business model is also quite prevalent in the real world (particularly among lawyers): it is known as the kickback.

IV. CONCLUSION

Of late, the information sector has done a very good job at attracting the attention of law makers. That is why so many new intellectual property rights have been recognized. The time has come for this community—especially this Valley—to think about whether things have gone far enough, whether privatization is starting to chill innovation rather than promote it. As to business method patents in particular, there is an expression about throwing the baby out with the bath water. Perhaps what we are dealing with here is the opposite situation: we are keeping the bath water (business method patents) when all we really need or want is the baby (patents on software).

COMMENTS

Surfing the Web for Capital: The Regulation of Internet Securities Offerings

Jonas A. Marson[†]

TABLE OF CONTENTS

The Internet[1] is having a profound effect on all parts of the securities business: web sites are linking small companies with angel investors[2]; growing companies are selling securities directly to the

[†] Law Clerk to the Honorable Samuel Conti, U.S. District Court for the Northern District of California. J.D. Harvard Law School, 1999; M.Sc. London School of Economics and Political Science, 1996; A.B. Harvard College, 1995.

1. Originally designed by the military to help computer scientists and engineers working on military projects communicate with one another, the loose collection of transmission lines, routers, and servers that comprise the Internet has now become a mass communication medium used by business, universities, individuals, and the government. Information is transmitted over the Internet via the World Wide Web, electronic mail, and electronic bulletin boards. For a general survey on the rise of the Internet, see *The Accidental Superhighway*, ECONOMIST, July 1, 1995, at 50.

2. Angel investors generally are individual investors or groups of individual investors who invest money in companies in exchange for stock when the company is not yet large enough to attract venture capital. Angel investors want a strong return on their investment, but may also has altruistic motivations as well. *See* Gwyneth E. McAlpine, *Getting a Piece of the Action: Should Lawyers be Allowed to Invest in their Clients' Stock?*, 47 UCLA L. REV. 549, 571-72 (1999).

public over the Internet; large publicly traded corporations are conducting "roadshows" over the Internet and distributing annual reports, prospectuses, and proxy materials via their web sites; and retail investors are routinely trading securities using on-line services.[3] Each of these developments has raised a host of legal issues. The U.S. Securities and Exchange Commission (the SEC) must, in response, apply and adapt a regulatory framework that was created almost seven decades ago by the Securities Act of 1933 (the "Securities Act")[4] and the Securities Exchange Act of 1934 (the "Exchange Act")[5] to a securities industry that is rapidly integrating the Internet into its everyday practice.[6] How it chooses to do so could have a profound affect on the future development of the capital raising process in the United States.

Congress passed the securities laws in response to the activities culminating in the 1929 market crash. The legislation created a regulatory scheme designed to ensure that securities offerings, as well as the listing and registration for public trading of such securities on a securities exchange, were accompanied by full disclosure of relevant information to the investing public. Under the Securities Act, companies intending to sell securities to the public must register the securities by filing a registration statement with the SEC.[7] The registration statement, which includes the statutory prospectus sent to investors, contains the information about the company and the

3. For general discussions on the rise of Internet web sites involved in securities offerings, see Constance E. Bagley & Robert J. Tomkinson, *Internet is Seeing its Share of Securities Offerings*, NAT'L L. J., Feb. 2, 1998, at C3 (predicting that the Internet will become an alternative to traditional means of raising capital); Richard Raysman & Peter Brown, *Securities Offerings Over the Internet*, N.Y. L.J., June 10, 1997, at 3 (noting that Internet-based securities offerings are likely to increase, especially for smaller companies that do not have access to institutional investors or venture capital). *But see* Andrew Reinbach, *Internet IPOs: Hip or Hype?*, AM. BANKER, Nov. 10, 1997, (Future Banker Magazine), at 40 (arguing that the attention given to Internet-based offerings is much larger than their actual performance, and that most large banks are unlikely to participate due to high risks and low returns).

4. Ch. 38, 48 Stat. 74 (1933) (codified as amended at 15 U.S.C.A. § 77a–77aa (West 1997 & Supp. 1999)).

5. Ch. 404, 48 Stat. 881 (1934) (codified as amended at 15 U.S.C.A. § 78a–78mm (West 1997 & Supp. 1999)).

6. A central question in many areas of the law is whether existing legal regimes can be adapted to the problems presented by new technologies or whether new regimes will need to be created. On this issue as it relates to securities regulation and the Internet, see Robert A. Prentice, *The Future of Corporate Disclosure: The Internet, Securities Fraud, and Rule 10b-5*, 47 EMORY L.J. 1, 7 (1998) (arguing that existing antifraud statutes and rules can be adapted to Internet abuses).

7. *See* 15 U.S.C.A. § 77e(a), (c) (West 1997).

offering that investors would need to properly evaluate the security.[8] This paper focuses principally on the ways in which these registration and disclosure requirements of the Securities Act apply to offerings conducted over the Internet, the relevant exemptions from these requirements, and the potential effect of recent reform efforts on Internet-based securities offerings.

Part One reviews the current approach to the regulation of Internet-based securities offerings. It first examines the SEC's approach to securities offerings conducted over the Internet that are exempt from the registration requirements of the Securities Act. It then examines the regulation of registered public offerings, focusing on the requirements for electronic delivery of information. Finally, it analyzes the rules regarding Internet-based roadshows. Part Two examines the SEC's most recent reform proposal, "The Aircraft Carrier Release," so-called because of its enormous size. It first reviews the basic provisions of the Release, and then highlights the probable impact of the proposed changes on Internet-related securities offerings. Part Three concludes, arguing first that the Release provides insufficient guidance to companies conducting exempt offerings over the Internet and, second, that the Release should be revised, specifically by eliminating the requirement that "free writings" be filed with the SEC, so as to encourage the use of the Internet as a means for information delivery.

I. CURRENT LAW

A. Exempt Offerings

Small companies face disproportionately high expenses in a registered public securities offering because many of the activities required by the securities laws, such as putting together a prospectus and mailing information to investors, are relatively fixed costs. In addition, because they have never accessed the public markets before, compliance with the disclosure requirements of the securities laws often requires small companies to reorganize their capital structure, employ auditors, and gather significant amounts of information about the company for the first time. Thus, the costs of a registered public securities offering may be far too great for a small or growing company that requires only a minor amount of capital.[9]

8. *See* 15 U.S.C.A. § 77g, aa (West 1997 & Supp. 1999).

9. *See* Stephen J. Choi, *Gatekeepers and the Internet: Rethinking the Regulation of Small Business Capital Formation*, 2 J. SMALL & EMERGING BUS. L. 27, 29 (1998).

Fortunately, these companies can take advantage of several exemptions from the registration requirements of the federal securities laws. In particular, section 3(b) of the Securities Act authorizes the SEC to add any class of securities to the general list of those exempted by section 3, subject to certain restrictions, provided that the aggregate amount offered is less than $5 million.[10] Exemptions under section 3(b) include Regulation A[11] and Regulation D, Rules 504 and 505.[12] In addition, section 4(2) provides a private placement exemption for transactions not involving any public offering.[13] Regulation D, Rule 506 provides a safe harbor under this Section for offerings of unlimited size, provided that they are sold only to accredited[14] or sophisticated[15] investors, and that sales are not made to more than thirty-five non-accredited investors.[16] Offerings under Rules 505 and 506 must meet the general conditions of Rule 502, including a prohibition on general solicitation and advertising, information and delivery requirements, and limitations on resale.[17]

1. Regulation D and General Solicitation — Issuers conducting offerings over the Internet relying on the exemptions under Rules 505 or 506 of Regulation D must be careful not to engage in general solicitation or advertising prohibited by Rule 502(c). The SEC has made it clear that, in the context of an exempt offering, the placement of offering materials on an Internet web site without sufficient procedures to limit access to accredited investors is inconsistent with the prohibition against general solicitation or advertising.[18] For example, if a company raising money through a private placement pursuant to Rule 506 simply placed its offering materials on its Internet site without restricting access to the materials beyond

10. *See* 15 U.S.C.A. § 77c(a), (b) (West 1997).

11. *See* Securities Act Rules, 17 C.F.R. §§ 230.251–230.263 (1999).

12. *Id.* §§ 230.504, 230.505.

13. *See* 15 U.S.C.A. § 77d(2) (West 1997).

14. Accredited investors include individuals with a net worth exceeding $1 million dollars or an annual income exceeding $200,000 (or $300,000 including the individual's spouse), as well as various institutions such as banks, broker-dealers, and insurance companies. *See* Securities Act Rules, 17 C.F.R. § 230.501(a) (1999).

15. A sophisticated investor is an investor having "such knowledge and experience in financial and business matters that he is capable of evaluating the merits and risks of the prospective investment." Such an investor may be sophisticated alone or with a purchaser representative. *See id.* § 230.506(b)(ii).

16. *See id.* § 230.506.

17. *See id.* § 230.502.

18. *See* Use of Electronic Media for Delivery Purposes, Securities Act Release No. 33,7233, Fed. Sec. L. Rep. (CCH) ¶3,200, at 3131-7 (Oct. 6, 1995) (hereinafter October Release).

requiring certain information, it would be engaging in prohibited general solicitation.[19] Therefore, if an on-line service is involved in offerings exempt under Rules 505 or 506 of Regulation D, it must place restrictions on the ability of potential investors to view such material, or it must otherwise locate prospective purchasers without a general solicitation.

In a no-action letter to IPONet, the SEC's Division of Corporation Finance approved a restricted access web site as consistent with the prohibition of general solicitation and advertising under Regulation D in the context of Internet-based private offerings.[20] Persons who have registered with IPONet can request registration as an accredited or sophisticated investor by filling out an on-line questionnaire designed to allow the company to determine whether the member is an accredited investor within the meaning of Rule 501(a) of Regulation D or a sophisticated investor under Rule 506. Once a member is qualified as either an accredited or sophisticated investor, he is given a password allowing him access to a restricted page where private offerings are posted.[21] The Division of Corporation Finance wrote that the qualification of investors through the use of a questionnaire would not constitute general solicitation or advertising provided that three conditions were met: (1) both the invitation to complete the questionnaire and the questionnaire itself do not reference any specific transactions posted or to be posted on the password protected page; (2) the password protected page is only available to an investor after the company has determined that he is accredited or sophisticated; and (3) the investor is only able to purchase securities in transactions that are posted after the investor is qualified with IPONet.[22] Thus, the posting of a notice of a private offering on a web site would not be deemed a public solicitation or general advertisement within the meaning of Regulation D when pre-qualification and password-protection procedures designed to limit access to the web site to accredited and sophisticated investors are in place.

The purpose of the IPONet no-action letter's third condition, that investors can only purchase securities posted after the investor has been qualified, is to ensure that investors do not join an on-line

19. *See id.* at 3131-7.

20. *See* IPONet, SEC No-Action Letter, [1996 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,252, at 77,270 (July 26, 1996).

21. *See id.* at 77,272.

22. *See id.* at 77,274.

service in order to invest in a particular offering. The SEC further refined this condition in its no-action letters to Lamp Technologies, Inc. ("Lamp").[23] Lamp lists descriptive information and performance related data from hedge funds[24] that are privately offered pursuant to Regulation D.[25] Subscribers to the password protected site—generally sophisticated investment and financial professionals—are pre-qualified by Lamp as accredited investors through the use of a questionnaire.[26] Because hedge funds have continuous quarterly or annual sales, rather than requiring investors to invest only in funds posted after their qualification, Lamp imposes a thirty-day waiting period during which time subscribers cannot invest in any posted hedge fund (other than funds in which the subscriber already invests, for which he has already been solicited, or in which he is already actively considering an investment).[27] The Division of Corporation Finance approved this procedure, noting that Lamp would not be considered to be engaging in general solicitation or advertising provided it meets the first two conditions of the IPONet no-action letter and enforces its thirty-day waiting period in lieu of the condition that investors can only purchase securities posted after the investor has been qualified.[28]

The opportunity for small companies to directly tap capital sources by using the Internet rather than traditional investment advisory services has produced a phenomenon recently dubbed "technological disintermediation."[29] Until recently, in order not to violate the prohibition on general solicitation, small companies had to

---

23. *See* Lamp Technologies, Inc., SEC No-Action Letter, [1998 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,453, at 78,327 (May 29, 1998) (hereinafter 1998 Lamp Letter); Lamp Technologies, Inc., SEC No-Action Letter, [1997 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,359, at 77,804 (May 29, 1997) (hereinafter 1997 Lamp Letter).

24. Hedge funds are largely unregulated private investment companies, usually in the form of partnerships, limited liability companies, or offshore corporations, that use a variety of alternative investment techniques, such as short-selling and derivatives. They may or may not use "hedging" strategies. *See* Leon M. Metzger, *Recent Market Events and the Foundation for Global Market Crises: Hedge Funds*, 4 FORDHAM FIN. SEC. & TAX L.F. 5, 6 (1999).

25. *See* 1997 Lamp Letter, *supra* note 23, at 77,805.

26. *See id.*

27. *See id.* at 77,806.

28. *See id.* at 77,809; 1998 Lamp Letter, *supra* note 23, at 78,330.

29. *See* Donald Langevoort, *Angels on the Internet: The Elusive Promise of "Technological Disintermediation" for Unregistered Offerings of Securities*, 2 J. SMALL & EMERGING BUS. L. 1, 2-3 (1998) (noting that "[t]echnology raises the promise of a substantially disintermediated capital market for start-up business, wherein entrepreneurs are able to solicit capital without having to pay underwriters or broker-dealers for marketing services, or lawyers and accountants for the heavy expenses associated with a registered public offering.") (footnote omitted).

undergo the cumbersome and expensive task of first finding qualified investors, and then after some period of time contacting them with a specific investment proposal.[30] This process would almost always require the assistance of an investment professional or registered broker-dealer[31] that had already compiled a list of pre-qualified investors through mailings, telephone solicitations, or personal contacts.[32] With the rise of Internet-based systems like that of IPONet, however, companies can now directly access lists of prospective investors without the need for investment professionals.[33] Thus, technology has eliminated the need for the "intermediary." Proponents of this phenomenon have argued that it substantially reduces the costs of raising capital for small businesses who can reach a large audience of potential investors without having to pay broker-dealers fees for marketing their company, and without having to sacrifice the extensive legal, accounting, and investment banking costs associated with a registered offering.[34]

2. Information Delivery and the Number of Purchasers — Other potential problems that could arise should an on-line service participate in offerings under Rules 505 or 506 of Regulation D without restricting access to accredited investors relate to information delivery requirements and restrictions on the number of purchasers. Rule 502(b) requires that certain information be furnished if issuers

30. *See id.* at 7.

31. Section 3(a)(4) of the Exchange Act defines a broker as "any person engaged in the business of effecting transactions in securities for the account of others." 15 U.S.C.A. § 78c(a)(4) (West 1997). Under § 3(a)(5) of the Exchange Act, a dealer is "any person engaged in the business of buying and selling securities for his own account, through a broker or otherwise." *Id.* § 78c(a)(5). By collecting orders and executing them in the various securities markets, broker-dealers facilitate securities trading. Exchange Act § 15(a) requires brokers and dealers to register with the SEC. *See id.* § 78o(a).

32. *See* Langevoort, *supra* note 29, at 7.

33. *See id.* at 7–8.

34. *See id.* at 3. Critics of the disintermediation of capital markets have argued that the process compounds information asymmetry problems between investors and companies and, by allowing small firms to shift their sources of capital from traditional financing methods (such as bank loans, venture capital, and angel investors) to public capital markets, the process increases monitoring costs. *See, e.g.*, Bernard Black, *Information Assymmetry, the Internet, and Securities Offerings*, 2 J. SMALL & EMERGING BUS. L. 91, 91 (1998) (arguing that "the Internet could increase information asymmetry costs by undercutting the effectiveness of the institutions that today provide investors with partial assurance of the quality of the information provided by issuers."); Jill Fisch, *Can Internet Offerings Bridge the Small Business Capital Barrier?*, 2 J. SMALL & EMERGING BUS. L. 57, 57 (1998) (arguing that there are "nonfinancial benefits that banks and private equity provide to small businesses through active managing and monitoring" and that "[s]hifting the source of small business capital may sacrifice these benefits, at the costs of future business performance.").

sell securities under Rules 505 or 506 to non-accredited investors.[35] If the on-line service is acting as a broker-dealer and selling the securities itself, such information would need to be furnished to everyone accessing the site, since there would be no way to determine whether the person purchasing such securities is accredited or not. If the on-line service is merely posting the offering materials and requires an investor to contact the issuer directly to purchase any securities, the service could presumably rely on the issuer to provide the required information before conducting a sale. However, because Rule 502(b)(1) requires such information to be provided to all non-accredited investors "a reasonable time prior to sale," it is safer to furnish the information initially on the web site.[36]

Rules 505(b)(2)(ii) and 506(b)(2)(i) require offerings to be limited to no more than thirty-five non-accredited investors.[37] Depending on how the on-line service functions, a service selling securities may not be able to restrict sales to only thirty-five non-accredited investors. Furthermore, even if it could, the service may be forced to unduly restrict the number of potential sales by selling to a total of only thirty-five purchasers (whether accredited of not) to prevent violating the limitation on the number of non-accredited investors. Again, a service merely providing information could presumably rely on the issuer to determine accredited status and restrict the number of sales to non-accredited investors to thirty-five.

3. Regulation A — Regulation A provides an exemption from registration for offerings of up to $5 million, imposes no limits on the number of offerees or purchasers, and authorizes the use of some forms of advertising.[38] Issuers taking advantage of Regulation A must, however, file an "offering statement" with the SEC, which includes an "offering circular" that must be delivered to purchasers prior to sale.[39] Regulation A offerings have been dubbed "minipublic" offerings because the information required to be disclosed in the offering statement is similar to, though far less extensive than, that mandated to be included in a registration statement.[40]

Because Regulation A offerings (as well as those conducted

35. *See* Securities Act Rules, 17 C.F.R. § 230.502(b) (1999).
36. *Id.* § 230.502(b)(1).
37. *See id.* § 230.505(b)(2)(ii), 230.506(b)(2)(i).
38. *See id.* § 230.251.
39. *See id.*
40. *See* MARC STEINBERG, UNDERSTANDING SECURITIES LAW 54–55 (2nd ed. 1996).

pursuant to Rule 504 of Regulation D) are not subject to restrictions on public solicitations or advertising, some web sites involved in Internet-based offerings have limited the types of unregistered offerings they post to those exempt under Regulation A. For example, in its request for no-action letter assurance, the Internet Capital Corporation ("ICC") explained that it does not list offerings exempt under Rules 505 or 506.[41] ICC's user registration process only requires that the potential investor provide his name, address, state of residence, and electronic mail address. While ICC will validate this information, unlike IPONet it has no procedure for determining whether an investor is accredited or not.[42] In a no-action letter, the Division of Corporation Finance approved this electronic posting of offering materials.[43]

A second attractive feature of Regulation A is the fact that issuers are allowed to "test the waters" to determine if there is any potential investor interest in a proposed offering. Specifically, issuers can publish or deliver "solicitations of interest" to potential investors consisting of oral communications, written documents, or radio or television broadcasts about the company and the offering.[44] This ability to "test the waters" has made Regulation A particularly attractive to small companies intending to sell securities directly to the public without the aid of an underwriter in so-called "direct public offerings." For example, Spring Street Brewing Company, which conducted the first ever Internet-based direct public offering, placed an offering circular complying with the requirements of Regulation A on its web page along with an investor subscription agreement that investors could complete and return with a check to purchase securities from the company. The company raised $1.6 million and avoided underwriting fees entirely.[45]

B. Registered Public Offerings

The SEC has generally encouraged the use of electronic distribution methods for transmitting required information to

41. *See* Internet Capital Corp., SEC No-Action Letter, 1997 WL 796944 (S.E.C.), at *1 (Dec. 18, 1997). ICC posts both registered and unregistered offerings. However, the only unregistered, i.e. exempt, offerings it posts are Regulation A and SCOR offerings. *See id.*

42. *See id.* at *3-*4.

43. *See id.* at *5.

44. *See* Securities Act Rules, 17 C.F.R. § 230.254 (1999).

45. *See* Christina K. McGlosson, *Who Needs Wall Street? The Dilemma of Regulating Securities Trading in Cyberspace*, 5 COMMLAW CONSPECTUS 305, 307 (1997); Jeffrey Taylor, *SEC Says Brewery May Use Internet to Offer Its Stock*, WALL ST. J., Mar. 26, 1996, at C1.

investors, and clearly expects the use of electronic media to grow in popularity in the securities industry. One reason for this inevitable growth is that the preparation and delivery of documents in a registered public offering, from the prospectus to sales literature and research material, can be accomplished at significantly less cost by using the Internet rather than traditional paper-based methods.[46] Other benefits of electronic delivery include much greater speed and the leveling effect of ending the current two-tiered system of disclosure that often allows larger institutional shareholders to receive information before smaller retail investors.[47]

Section 5(b)(2) of the Securities Act requires that a prospectus containing the salient data set forth in the registration statement be delivered to any investor purchasing a security either before or at the time of sale.[48] This requirement is designed to ensure that investors are given the information they need to properly evaluate the security and to make an informed investment decision. Thus, a central question is to what degree issuers can rely on the Internet to meet this disclosure obligation by transmitting the required information electronically.[49] The SEC's general approach is that information distributed through electronic means satisfies the transmission requirements of the securities laws as long as the intended recipients receive substantially the same information as they would have received if the information had been delivered to them in paper

46. *See* McGlosson, *supra* note 45, at 315.

47. *See* Catherine M. Kilbane, *Prospectus Delivery via the Internet,* 8 CORP. ANALYST 62, 63–64 (1996). Institutional investors, by virtue of the fact that they usually possess "significant assets and expertise," are generally assumed to be in a position to demand information from issuers similar to what might be included in a registration statement. Kenneth Denos, *Blue and Gray Skies: The National Securities Markets Improvement Act of 1996 Makes the Case for Uniformity in State Securities Law,* 1997 UTAH L. REV. 101, 120 (1997). Such institutional investors include insurance companies, various forms of investment companies, pension plans, dealers, investment advisors, and certain charitable organizations. *See id.* at 121. Already some leveling has been accomplished by the SEC's web site. *See* David M. Cielusniak, *You Cannot Fight What You Cannot See: Securities Regulation on the Internet,* 22 FORDHAM INT'L L.J. 612, 617 (1998) (noting that the use of EDGAR for Exchange Act filings has made extensive financial information about public companies instantly available to any investor via the SEC's web site).

48. Section 5(b)(2) of the Securities Act makes it unlawful to "carry or cause to be carried through the mails or in interstate commerce any such security for the purpose of sale or for delivery after sale, unless accompanied or preceded by a prospectus that meets the requirements of subsection (a) of section 10." 15 U.S.C.A. § 77e(b)(2) (West 1997).

49. The SEC outlined its approach to electronic delivery in two releases. *See* October Release, *supra* note 18 at 3128; Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, Securities Act Release No. 33,7288, Fed. Sec. L. Rep. (CCH) ¶ 3,201 at 3131-12 (May 9, 1996) (hereinafter May Release).

form.[50] This section reviews the SEC's three guiding principles for electronic delivery: notice, access, and evidence of delivery.

1. Notice — Parties using electronic delivery must ensure that their electronic communication provides timely and adequate notice to investors that information regarding a proposed offering is publicly available. While the delivery of an electronic document itself (such as a CD-ROM or an electronic mail) constitutes sufficient notice, posting a document on an Internet web site, without separate notice, does not satisfy the delivery requirements.[51] In general, notice by publication in a newspaper, bulletin board, or web site is also insufficient.[52]

If, however, an investor has consented to electronic delivery via a web site, a note with the confirmation of sale of the security indicating that the final prospectus is available on a web site is sufficient to satisfy the delivery requirements.[53] Moreover, if such an investor has provided his or her electronic mail address for the purpose of being notified, an issuer may send notice of the location of the final prospectus via electronic mail.[54] Assuming again that an investor has consented to electronic delivery, notice can be given by including in the forepart of a company's sales literature a clearly highlighted provision indicating the availability on an Internet web site of the final prospectus.[55]

2. Access — Electronically delivered information must provide investors with comparable access to the required disclosure information as would a conventionally delivered paper document.[56] Thus, the electronic medium cannot be "so burdensome that intended recipients cannot effectively access the information provided."[57] For example, if an investor must navigate through a confusing series of

50. *See* October Release, *supra* note 18, at 3131.

51. *See id.* at 3131-2.

52. *See id.* at 3131-7. In some circumstances, the issuer will be able to show that delivery to an investor has been satisfied by other means or that the document is not required to be delivered. For example, in an offering, neither notice of the availability of an updated or final prospectus nor the updated or final prospectus itself need be sent, through any means, to persons who have already received an electronic preliminary prospectus, but to whom securities are not expected to be sold. *See id.* at 3131-2 n.23.

53. *See id.* at 3131-3. Investors who have not consented to electronic delivery via a web site cannot be presumed to be able to access the web site; thus, a note indicating availability of the final prospectus on the web site is insufficient without such consent. *See id.*

54. *See id.* at 3131-5.

55. *See id.* at 3131-6.

56. *See* October Release, *supra* note 18, at 3131-2.

57. *Id.*

menus to access a document so that it is unreasonable to expect the investor to gain access, the procedure would be viewed as too burdensome and delivery would not be deemed to have occurred.[58] However, a procedure for ensuring access to prospectuses and other material that serves to limit access to all the materials to those with user identification numbers (even if the process of getting an identification number requires significant information and time from the investor) is not considered to be overly burdensome.[59] Such burdens are considered to be "part of the process of providing access to all the information, including supplemental sales literature, and not to be a unique burden upon access to the prospectus."[60]

On-line viewing is not a "prerequisite to electronic delivery."[61] Thus, a prospectus made available on the Internet that requires downloading of the entire document can still satisfy the delivery requirement.[62] In any case, since the investor must have the opportunity individually to "retain the information or have ongoing access equivalent to such personal retention," an issuer should at least allow, and perhaps even require, an investor to download the information.[63] "[T]he document should also be accessible for as long as the delivery requirement applies."[64]

Documents required to be accompanied by one another must each be as accessible as the other. Consider a web site that contains a prospectus and an application for a mutual fund as two separate files that can be downloaded independently. If an investor must download special software to view the prospectus but not the application, even a statement in a returned and completed application that the investor received the prospectus is insufficient to evidence electronic delivery of the prospectus.[65] On the other hand, if "it is not significantly more burdensome to access the prospectus than the application form (e.g., no additional software is necessary to read either document . . . .)," and the user downloads them together (even if they become two

58. *See id.* at 3131-2 n.24.

59. *See id.* at 3131-10.

60. *Id.*

61. *Id.* at 3131-11.

62. *See* October Release, *supra* note 18, at 3131-10 to 3131-11.

63. *Id.* at 3131-2.

64. *Id.* at 3131-2. In general, the prospective delivery requirement for sales other than from an unsold allotment lasts for 25 days after the offering date, which is defined as the date on which the registration statement becomes effective or the date on which the securities were bona fide offered to the public. *See* Securities Act Rules, 17 C.F.R. § 230.174 (1999).

65. *See* October Release, *supra* note 18, at 3131-9.

separate files on his computer), "electronic delivery of the prospectus can be inferred" from the returned application form.[66]

Last, because of possible system failures, incompatibilities, and revocations of consent, issuers must be able to deliver a paper version of documents delivered electronically.[67] In particular, an issuer must provide a paper version of a document if a person revokes his consent to receive a document electronically or specifically requests a paper version.[68] The SEC noted that this requirement should not preclude an issuer from structuring its offering through only electronic communication, but cautioned that the issuer must still deliver information through paper if electronic means can no longer be relied upon to deliver information required to be provided by the securities laws.[69]

3. Evidence to show delivery — Issuers or broker-dealers can obtain direct evidence that a particular investor actually received required disclosures by electronic mail, return receipts, or by confirmation that the investor accessed, downloaded, or printed the document.[70] Direct evidence of receipt may also be obtained through evidence that an investor has used other materials that are only available once the investor has already accessed the required disclosure information.[71] However, obtaining an informed consent from an investor stating that the investor specifically consents to receive information through a particular electronic medium obviates the need to produce direct evidence of delivery altogether.[72] Informed consent requires that investors be apprised of the particular electronic medium to be used (e.g., a web site), potential costs (such as on-line time), and "the period during and documents for which the consent will be effective."[73]

Even without an explicit consent, the SEC has made it clear that an investor accessing a required document via the Web can evidence

66. *Id.*

67. *See id.* at 3131-2.

68. *See id.* An investor need not withdraw his consent to request a paper copy of a document. *See id.* at 3131-8.

69. *See id.* at 3131-2 n.27.

70. *See id.* at 3131-3.

71. *See* October Release, *supra* note 18, at 3131-3.

72. *See id.*

73. *Id.* at 3131-3 n.29. An issuer can rely on a consent given to an underwriter, brokerage firm, or other service provider, and vice versa. *See id.* Such a consent must, however, specifically indicate that the investor consents to delivery of future documents by the particular electronic medium. *See id.* at 3131-4.

delivery of the required document.[74] For example, because sales literature must be preceded or accompanied by a final prospectus, such material, if placed on a web site, must include a hyperlink to the final prospectus.[75] In this case, "the hyperlink function enables the final prospectus to be viewed directly as if it were packaged in the same envelope as the sales literature,"[76] a notion called the "envelope theory."[77] Alternatively, sales material can be placed on the same menu as the prospectus as long as the two are clearly identified and in close proximity to one another.[78]

The SEC's analogy between two hyperlinked documents and the inclusion of the two documents in the same envelope can create pitfalls for issuers. For example, during the "waiting period," the time between the filing of the registration statement and the date on which it is deemed effective, section 5(b)(1) prohibits any written communications relating to the security offering unless made through the use of a prospectus conforming to the strict informational requirements of section 10.[79] Thus, issuers must be careful not to provide direct access via a hyperlink from their preliminary prospectus to research reports since such reports most certainly do not meet the information requirements of section 10.[80] In several no-action letters, the SEC has allayed issuers' concerns that the reference in a prospectus to an issuer's filings on its web site would incorporate by reference all other material on the site, such as marketing material.[81] An issuer may, therefore, include in its prospectus a statement such as, "'our SEC filings are also available to the public

74. *See id.* at 3131-4.

75. *See id.* at 3131-6.

76. *Id.*

77. *See* October Release, *supra* note 18, at 3131-6. The envelope theory seems only to apply to hyperlinks, and not to less speedy connections between documents. For example, a web site that allows a user to click on a box displayed in the supplemental sales literature to have the prospectus downloaded or to request that one be mailed, but does not allow the prospectus to be viewed on-line, "would not satisfy the prospectus delivery requirement... [b]ecause the system does not give users reasonably comparable access to the prospectus and the sales literature...." May Release, *supra* note 49, at 3131-23.

78. *See* October Release, *supra* note 18, at 3131-5 to 3131-6.

79. Section 5(b)(1) of the Securities Act makes it unlawful to "transmit any prospectus relating to any security with respect to which a registration statement has been filed... unless such prospectus meets the requirements of section 10." 15 U.S.C.A. § 77e(b)(1) (West 1997).

80. *See* October Release, *supra* note 18, at 3131-6.

81. *See* ITT Corp., SEC No-Action Letter, [1997 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,340, at 77,701 (Dec. 6, 1996); Baltimore Gas and Elec. Co., SEC No-Action Letter, 1997 WL 6170 (S.E.C.), (Jan. 6, 1997).

from our web site,'"[82] without incorporating information other than the Exchange Act filings, such as documents available through hyperlinks from the company's main site.[83]

C. *Internet Roadshows*

Roadshows have become an integral part of securities offerings. Roadshows usually consist of a series of meetings at which the issuer's management makes presentations to institutional investors, securities firms, trading and sales personnel, and research analysts. A roadshow allows the underwriters to present information concerning the merits of the upcoming securities offering and the future prospects of the issuer, and provides an opportunity for potential investors to ask questions.[84] Roadshows take place during the waiting period.[85] During this period, section 5(b)(1) of the Securities Act prohibits the use of any prospectus other than a prospectus meeting the informational requirements of section 10 in order to market the securities.[86] Section 2(a)(10) defines a prospectus broadly as any "prospectus, notice, circular, advertisement, letter, or communication, written or by radio or television, which offers any security for sale."[87] Since roadshows are essentially oral presentations, they do not fall within this statutory definition of a prospectus, and are thus not subject to section 5(b)(1). Until recently, however, the reference to radio and television in section 2(a)(10) foreclosed the use of electronic communications to transmit oral roadshows for fear that such communications would be considered prospectuses.[88]

In a no-action letter to Private Financial Network ("PFN"),[89] the

---

82. Baltimore Gas, *supra* note 81, at *2.

83. *See id.*

84. *See generally* Mark Leibovich, *Journey Into the Secret Heart of Capitalism: Cross-Country "Roadshow" Marks a Young CEO's Stock Market Debut,* WASH. POST, Aug. 9, 1998, at A1 (account of high technology company roadshow).

85. Roadshows cannot be conducted in the "pre-filing period," the time before a registration statement has been filed, because § 5(c) of the Securities Act prohibits all offers to sell a security unless a registration statement has been filed with the SEC. 15 U.S.C.A. § 77e(c) (1997). The term "offer to sell" is broadly defined in § 2(3) of the Securities Act to include "every attempt to offer or dispose of" a security, and has been interpreted broadly to include any publicity intended to condition the market for a public offering. *See* HAROLD S. BLOOMENTHAL ET AL., SECURITIES LAW HANDBOOK § 5.01(2) (1999).

86. *See* 15 U.S.C.A. § 77e(b)(1) (West 1997).

87. *Id.* § 77b(a)(10).

88. *See* Linda C. Quinn & Ottilie L. Jarmel, *The Road Less Traveled: The Advent of Electronic Roadshows,* INSIGHTS, July 1997, at 3 (discussing Internet roadshows in the context of the Private Financial Network no-action letter, see *infra* note 89 and accompanying text).

89. PFN, a subsidiary of the MSNBC joint venture between NBC and Microsoft, provides

Division of Corporation Finance approved PFN's proposal to transmit roadshow presentations to its subscribers via satellite, T1 telephone lines, and cable under the assumption that such communications would not fall under the definition of a prospectus within the meaning of § 2(a)(10) of the Securities Act.[90] PFN argued that an electronic roadshow would not lose its character as an "oral" presentation merely because it is transmitted over the same technology as radio or television.[91] Indeed, the reference to radio and television in § 2(a)(10), PFN argued, was "intended to prevent mass communications to the public unaccompanied by the sort of disclosure required § 10."[92] Citing *Gustafson v. Alloyd Co., Inc.*,[93] PFN argued that the term "prospectus" was only meant to refer to communications widely disseminated to the public rather than to a smaller, invited audience.[94] The SEC granted the no-action letter with little commentary.[95]

Subsequently, the SEC has granted several no-action letters to other companies providing electronic roadshows. In particular, the Commission has provided no-action letters to two companies transmitting roadshow presentations over the Internet: Net Roadshow and Thomson Financial Services' Virtual Roadshow.[96] Both services operate in much the same way as PFN, except that they broadcast their roadshow presentations over the Internet. On Net Roadshow's web site, anyone can view the list of roadshows and underwriters, but

---

video programming to about 100 subscribers--principally broker-dealers and investment advisors--who view the material, such as interviews with CEOs and project announcements, on their computer and television monitors. PFN proposed to transmit roadshows, in either a live or delayed format, in order to "help issuers channel timely and consistent information about themselves and their securities to potential investors who otherwise could attend the shows but might find it expensive or difficult to do so." Private Financial Network, SEC No-Action Letter, [1997 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,332, at 77,674 – 75 (Mar. 12, 1997).

90. *See id.* at 77,678.

91. *See id.* at 77,676.

92. *Id.* at 77,677.

93. 513 U.S. 561 (1995).

94. *See* Private Financial Network, *supra* note 89, at 77,677 – 78.

95. *See id.* at 77,678. PFN does take several steps to ensure compliance with the securities laws, such as making the transmissions available only to the network's subscribers, who must agree not to tape, copy, or further distribute the presentation, and insuring that each subscriber receives a prospectus before a roadshow is transmitted. In addition, PFN instructs issuers and underwriters to make sure that the information disclosed in the roadshow is not inconsistent with the information contained in the prospectus, and includes with each transmission a visual statements (or "crawl") emphasizing the primacy of the prospectus as well as the prohibition on copying and further distribution. *See id.* at 77,676 – 77.

96. *See* Net Roadshow, SEC No-Action Letter, [1997 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,367, at 77,849 (July 23, 1997); Thomson Financial Services, SEC No-Action Letter, 1998 WL 575139 (S.E.C.) (Sept. 4, 1998).

an investor who wishes to view a particular presentation must contact one of the underwriters to obtain an access code, which is changed each day to prevent multiple viewings.[97] Only qualified users with an identification number can access the Virtual Roadshow site's index of companies. In order to view a roadshow presentation, a user must also have received authorization from the underwriter, who has previously agreed to provide a copy of the prospectus to investors before granting them such authorization.[98] Although investors on Net Roadshow do not actually receive a paper prospectus before viewing the roadshow, investors are directed to access and download the prospectus through a prominently displayed button on the web page at any time before, during, and after the roadshow presentation.[99]

It is not entirely clear how far Internet-based roadshow providers can go in terms of expanding the audience for their presentations beyond institutional investors. On the one hand, if an electronic roadshow is by definition an oral communication, it should not matter how many or what kind of investors watch as long as adequate disclosure mechanisms are in place.[100] On the other hand, all of the services receiving no-action assurance so far restrict their web sites to the types of investors who are ordinarily invited to roadshows, such as institutional investors or research analysts.[101] Furthermore, a web site open to anyone could perhaps be analogized to broadcast media such as radio and television, which are explicitly part of the definition of a prospectus under section 2(a)(10), because any potential investor could "tune in." The SEC has taken a few tentative steps in the direction of expanding the potential base of investors able to access Internet roadshows, such as by issuing a no-action letter to the heavily subscribed Bloomberg service to conduct electronic roadshows.[102]

---

97. *See* Net Roadshow, *supra* note 96, at 77,849; *NetRoadshow* (visited Mar. 10, 2000) <http://www.netroadshow.com>.

98. *See* Thomson Financial Services, *supra* note 96, at *5-*6.

99. *See* Net Roadshow, *supra* note 96, at 77,849. Similarly, Virtual Roadshow's index has a hyperlink to the EDGAR system on the SEC's web page. *See* Thomson Financial Services, *supra* note 96, at *5.

100. *Cf.* Quinn & Jarmel, *supra* note 88, at 4 ("Moreover, there is no legal limitation on the number or nature of potential investors that may attend or participate in such meetings. A company, for example, could, consistent with the Securities Act, hold a roadshow at Yankee Stadium.").

101. For example, Net Roadshow's web site notifies visitors that "[t]he intended audience [for a roadshow presentation] is professional money managers, portfolio managers, research analysts, and those who would otherwise be permitted to attend the live roadshow." *NetRoadshow Frequently Asked Questions (FAQs)* (visited Mar. 12, 2000) <http://www.netroadshow.com/site/help/faqs.htm>.

102. *See* Bloomberg L.P., SEC No-Action Letter, 1997 WL 739085 (S.E.C.) at *5-*6 (Dec.

More recently, the SEC gave oral assurances to Net Roadshow that it could expand its service to accredited individual investors, allowing them to tap into the increasing number of retail investors who invest on-line.[103] The lack of guidance in this area, however, means that Internet roadshows may still be limited to certain types of investors, preventing the information contained in the presentations from directly reaching a broader audience.

II. PROPOSED CHANGES

The SEC has recently proposed significant changes to the regulatory framework established by the securities laws in what has been dubbed, "The Aircraft Carrier Release."[104] While past reform efforts have usually been precipitated by a major event, such as the depression of the 1930s or the insider trading scandals of the 1980s, the issuance of the Aircraft Carrier Release does not seem to have been driven by any one factor, though the rapid growth in information technology and the rise of the Internet in particular have played an important role in the SEC's recent shift toward the deregulation of information delivery requirements.[105] The SEC's stated goal of this reform effort is to increase the flexibility of registered offerings in terms of timing and disclosure without compromising investor protection.[106] To this end, the Aircraft Carrier Release proposes to streamline the registration process for securities offerings, especially for seasoned issuers, while at the same time increasing the application of antifraud and civil liability protections for investors.

A. Introduction to the Aircraft Carrier Release

The proposed reforms would replace the current registration

1, 1997); BLOOMENTHAL ET AL., *supra* note 85, at § 5.02(b) (concluding that the Bloomberg no-action letter implies that the number of viewers is not important to the SEC).

103. *See* Allyson Vaughan, *Firm Gets Approval from SEC to Include Individuals in Virtual Roadshows,* CORP. FINANCING WEEK, Feb. 9, 1999, at 1.

104. *See* Regulation of Securities Offerings, Securities Act Release No. 33,7606A, [1999 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 86,108, at 81,461-63 (Nov. 13, 1998) (hereinafter Reform Release).

105. *See "Aircraft Carrier" Sprouts Leaks,* INV. REL. BUS., Jan. 18, 1999 ("[T]he sweeping nature of the aircraft carrier proposal appears to be driven by the SEC's agenda, rather than a reaction to a major event."); Laura S. Unger, *The "Aircraft Carrier": Technological Implications and Unresolved Issues,* INSIGHTS, Jan. 1999, at 32 ("Technology--particularly the Internet--has made it easier to deliver information to investors. As a result, the Commission has rethought how improved information delivery impacts what information investors should have during the various stages of a securities offering.").

106. *See* Reform Release, *supra* note 104, § I(A), at 81,467.

statement forms with three new forms: Form A for small or unseasoned issuers; Form B for large, seasoned, and well-followed issuers or for offerings to sophisticated or informed investors; and Form C for business combinations and exchange offers.[107] Form B registration statements would be deemed effective at the issuer's request, and would not be reviewed in advance by the SEC staff.[108] Form B registration statements would also incorporate an issuer's Exchange Act filings by reference.[109] As a tradeoff for the added flexibility and control over timing, however, Form B registrants would be required to include all transaction information within the registration statement prior to the first sale rather than in a supplement after sales are already made.[110] Form B would generally be available only to issuers with a demonstrated market following.[111] However, to encourage the registration of offerings to institutions that would otherwise be exempt from registration under Securities Act Rule 144A, the SEC has also proposed that Form B be available for sales to "qualified institutional buyers."[112]

Issuers using Form A would have less flexibility than those using Form B. The rules governing effectiveness and incorporation depend, however, on whether an issuer is considered "seasoned" or not.[113]

---

107. *See id.* § V(A)–(D), at 81,474-505. The SEC has released a separate reform proposal relating to takeovers, which includes a detailed discussion of the regulation of business combinations and exchange offers. *See* Securities Exchange Act Release No. 34,40633, SEC Docket (Nov. 3, 1998).

108. *See* Reform Release, *supra* note 104, § V(A)(l)(d), at 81,478-79. In comparison, under the current system, it typically takes "several weeks to have a registration statement that is reviewed [by the SEC] declared effective." Marilyn Mooney & Gillian McPhee, *Aircraft Carrier Proposals Change the Timing Of the Registered Offering Process,* INSIGHTS, Jan. 1999, at 9.

109. *See* Reform Release, *supra* note 104, § V(A)(l)(a), at 81,475.

110. *See id.* § V(A)(1)(a)(ii), at 81,476-77. Such information is currently contained in a prospectus supplement under Securities Act Rules, 17 C.F.R. § 230.424(b) (1999). *See also* Mooney & McPhee, *supra* note 108, at 11.

111. *See* Reform Release, *supra* note 104, § V(A)(2)(a), at 81,481. Issuers considered to have such a market following must have both a history of reporting under the Exchange Act and either (1) a public float of between $75 and $250 million and an average daily trading volume of at least $1 million, or (2) a public float of above $250 million. *See id.* The SEC chose these criteria because it believes that they are "the most accurate measurement to attain the goal of choosing issuers for which there is an efficient market . . . ." *Id.*

112. *Id.* § V(A)(2)(b), at 81,482-83-84. Rule 144A provides an exemption from the requirements of Section 5 for the private resale of securities to certain institutions that are deemed to be "qualified institutional buyers," including insurance companies, employee investment plans, dealers, and banks. Securities Act Rules, 17 C.F.R. § 230.144A (1999).

113. For the purposes of allowing incorporation by reference, an issuer is considered to be seasoned if it has either (1) been a reporting company for at least two years and has a public float of over $75 million, or (2) has been a reporting company for at least two years and has

Issuers considered seasoned for the purposes of Form A would be able to incorporate their Exchange Act filings by reference into the prospectus in order to meet the company information disclosure requirements.[114] These Form A registration statements would also be deemed effective at the seasoned issuer's request.[115] Unseasoned issuers and those conducting initial public offerings, on the other hand, would have to provide company-related information in full in the prospectus, and their Form A registration statements would be declared effective only after SEC review on the timetable of current S-1 registration statements.[116]

The Aircraft Carrier Release would also significantly liberalize the rules restricting issuer communications during both the "pre-filing period," the time before the issuer files a registration statement, and during the waiting period. Currently, section 5(c) of the Securities Act prohibits offers during the pre-filing period (the "gun jumping" restrictions),[117] and section 5(b)(1) prohibits any written (though not oral) communications relating to a security offering during the waiting period unless made through the use of a prospectus conforming to the requirements of section 10(b).[118] Under the Aircraft Carrier Release, all restrictions on offering communications during the pre-filing period would be removed for Form B registrants, allowing such issuers to make offers before filing a registration statement.[119] Form A registrants could freely engage in offering communications up to the period starting thirty days before the date of filing of the registration statement.[120] Moreover, during this thirty day "cooling off" period, all Form A issuers could release "factual business communications" and reporting companies using Form A could release "regularly released forward-looking information" as well.[121] During the waiting period, the Aircraft Carrier Release would

---

filed at least two annual reports. *See* Reform Release, *supra* note 104, § V(B)(l)(a)(iii)(A), at 81,495. For the purposes of allowing issuers to choose the timing of the offering, an issuer is seasoned if it has a public float of at least $75 million or if the Exchange Act annual report incorporated into its registration statement has been reviewed by the SEC. *See id.* § V(B)(2)(a), at 81,496-97.

114. *See id.* § V(B)(l)(a)(iii), at 81,495.

115. *See id.* § V(B)(2)(a), at 81,496.

116. *See id.* § V(B)(l)(a)(iii)(B), at 81,496, V(B)(2)(b), at 81,498.

117. *See* 15 U.S.C.A. § 77e(c) (West 1997).

118. *See id.* § 77e(b)(1).

119. *See* Reform Release, *supra* note 104, § VII(A)(1)(a), at 85,517.

120. *See id.* § VII(A)(l)(c)(i), at 81,520-21.

121. *Id.* § VII(A)(1)(c)(ii), at 81,521-22. Factual business communications include information about the issuer, advertisements of the issuer's products or services, business or

allow issuers to make offers and communicate information in any form without having to meet the informational requirements of section 10.[122] However, issuers would be required to file all such "free writing material" with the SEC.[123]

In exchange for the accelerated timetable for offerings and increased flexibility regarding communications, the Aircraft Carrier Release clarifies and strengthens statutory antifraud and civil liability protections for investors. In particular, the Aircraft Carrier Release makes it clear that civil liability under section 11 of the Securities Act would apply to all information in the registration statement, including Exchange Act filings incorporated by reference.[124] In addition, civil liability under section 12(a)(2) of the Securities Act would apply to all free writing materials used in the offering period, including regularly released forward-looking information.[125] Furthermore, the antifraud protections under section 17(a) of the Securities Act and section 10(b) of the Exchange Act would attach to any communication that constitutes an offer or is in connection with the sale of a security, respectively, regardless of whether it was made during the offering period. Thus, communications made prior to filing (or prior to thirty days before filing for Form A registrants) would no longer technically constitute "offers" under the Aircraft Carrier's pre-filing period proposals.[126] Since the Reform envisions a

---

financial developments regarding the issuer, dividend notices, information in Exchange Act reports, and responses to unsolicited inquiries from stockholders, analysts, or the press, but do not include information about the offering itself. *See id.* § VII(A)(1)(c)(ii)(A) at 81,522. Regularly released forward-looking information must be usually released in the ordinary course of business, and includes such items as financial projections, statements of management's plans and objectives, and statements about future economic performance. *See id.* § VII(A)(1)(c)(ii)(B), at 81,522.

122. *See id.* § VII(A)(2), at 81,523.

123. *See id.* § VII(A)(2), at 81,524. "Free writings" generally refer to sales literature that is prohibited during the pre-filing and waiting periods.

124. *See id.* § V(C), at 81,499-502. Section 11(a) of the Securities Act attaches civil liability to issuers, underwriters, and accountants for "any part of the registration statement, when such part [becomes] effective, contain[ing] an untrue statement of a material fact or omitt[ing] to state a material fact required to be stated therein or necessary to make the statement therein not misleading." 15 U.S.C.A. § 77k (West 1997).

125. *See* Reform Release, *supra* note 104, § V(C)(2)(b), at 81,501. Section 12(a)(2) of the Securities Act provides civil liability against "any person who offers or sells a security... which includes an untrue statement of a material fact or omits to state a material fact necessary in order to make the statements, in light of the circumstances under which they were made, not misleading...." 15 U.S.C.A. § 77l(a)(2) (West 1997).

126. *See* Reform Release, *supra* note 104, § V(C)(2)(c), at 81,501. Section 17(a) of the Securities Act makes it unlawful for "any person in the offer or sale of any securities... to employ any devise, scheme, or artifice to defraud...." 15 U.S.C.A. § 77q(a)(1) (West 1997). Section 10(b) of the Exchange Act makes it unlawful "to use or employ, in connection with the

shift away from pre-effective review and toward further reliance by investors on incorporated Exchange Act filings (now readily available to most investors via EDGAR on the SEC's web site),[127] the Aircraft Carrier Release aims to improve the accuracy and completeness of these filings by requiring signatories of Exchange Act reports and registration statements to certify that the report or statement contains no material misstatement or omission. The Aircraft Carrier Release would also expand the group of persons required to sign several forms (including the 10-Q) to include the "principal executive officers of the registrant and a majority of the board of directors of the registrant."[128]

The Aircraft Carrier Release also aims to strengthen investor protection by re-focusing the prospectus delivery requirements from prospectus delivery at or before final confirmation of sale to prospectus delivery before the point in time when an investor has already made his investment decision. Section 5(b)(2) of the Securities Act requires issuers to send investors a final prospectus no later than the time of sale.[129] Though the SEC has adopted rules to give issuers an incentive to send a preliminary prospectus to investors earlier in the process, doing so is not required except under very limited circumstances.[130] The Aircraft Carrier Release would provide an exemption to the prospectus delivery requirement.[131] As a condition of the exemption, Form B registrants would be required to deliver either a term sheet or a preliminary prospectus containing transactional information before the investment decision is made, while Form A registrants would be required to deliver a preliminary prospectus three days before the security is priced or, in the case of an initial public offering, seven days before pricing.[132] Issuers would also have to inform investors by the time they have received

purchase or sale of any security registered on a national securities exchange or any security not so registered, any manipulative or deceptive device . . . ." 15 U.S.C.A. § 78j(b) (West 1997).

127. EDGAR stands for the Electronic Data Gathering, Analysis, and Retrieval system. EDGAR performs automated collection, validation, and indexing of submissions by companies required to file forms with the SEC and makes such information publicly available via the SEC's web site. *See EDGAR Database of Corporate Information* (last modified Feb. 22, 2000) <www.sec.gov/edgarhp.htm>.

128. Reform Release, *supra* note 104, § XI(C), at 81,566.

129. *See* 15 U.S.C.A. § 77e(b)(2) (West 1997).

130. *See, e.g.*, Securities Act Rules, 17 C.F.R. § 230.460 (1999) (allowing the SEC, when ruling upon requests for acceleration of effectiveness of a registration, to take into account whether the preliminary prospectus has been adequately distributed); Exchange Act Rules, 17 C.F.R. § 240.15c2-8 (1999) (requiring brokers and dealers to deliver a preliminary prospectus to investors 48 hours prior to confirmation of sale in the case of initial public offerings).

131. *See* Reform Release, *supra* note 104, § VIII(C)(3), at 81,536.

132. *See id.* § VIII(C)(4)(a)–(b), at 81,538.

confirmations of sale where they can acquire a final prospectus.[133] Investment banks have criticized the term sheet proposal, arguing that it will significantly slow down offerings by large issuers who currently can use the shelf registration system[134] to offer securities in a matter of hours.[135]

B. Effect of the Aircraft Carrier Release on Internet Securities Offerings

The rise of information technology was clearly an important factor in producing the Aircraft Carrier Release. Indeed, the SEC noted in the Release that, "[t]echnological innovations that permit instantaneous communications are a driving force behind this decade's securities market."[136] In addition, the SEC cites the increasing ability of investors to access information from corporate web sites and from company filings made publicly available on the SEC's own web site.[137] To encourage investors to make use of these resources, the Aircraft Carrier Release requires issuers to provide their web site address and an electronic mail contact on the cover page of registration statements filed under the Securities Act.[138]

Arguably the most important part of the Aircraft Carrier Release, in terms of its impact on the Internet, is the proposed removal of restrictions on communications during the pre-filing and waiting periods. One major impact of these changes relates to electronic roadshows. By eliminating the restriction that communications during the waiting period be limited to the preliminary prospectus, the Aircraft Carrier Release removes the need for electronic roadshow companies to receive no-action letter assurance that their individual system will not be deemed to violate section 5(b)(1) of the Securities Act.[139] In addition, the Aircraft Carrier Release would allow

133. *See id.* § VIII(C)(3)(a), at 81,536.

134. Shelf-registration allows securities to be offered or sold on a delayed or continuous basis. Specifically, Securities Act Rule 415 allows large issuers to file for offerings of equity securities that they plan to offer within two years of the effective date of the registration statement. *See* Securities Act Rules, 17 C.F.R. § 230.415 (1999).

135. *See* Charles Sisk, *Bankers Fret SEC Overhaul May Slow Down Offering Process*, CORP. FINANCING. WK., Feb. 22, 1999, at 1 (noting the claim by counsel for the Securities Industry Association that the term sheet requirement could delay shelf registration for days while issuers' and underwriters' lawyers examine term sheets for potential liabilities).

136. Reform Release, *supra* note 104, § VII(A)(1)(a), at 81,517.

137. *See id.* § V(A)(1)(a)(i), at 81,476.

138. *See id.* § VII(C), at 81,526.

139. *See New Rules Would End Road Show No-Action Requests*, FIN. NET NEWS, Nov. 23, 1998 at 6; *supra* Part I.C.

companies conducting electronic roadshows to communicate not only with institutional investors and analysts, but to retail investors as well.[140] The SEC seems to have placed a priority on broadening the audience for roadshows because of its understandable concern that roadshow presentations promote selective and unfair disclosure to a privileged few.[141] Though some have argued that selective disclosure does not hurt the investing public because information given to institutional or other large investors is quickly incorporated into the price of securities through their purchases and sales, the SEC at least believes that the retail market has been playing an important role in setting prices as well, especially with high technology stocks.[142] Finally, the proposal would allow issuers to accompany the roadshow presentation with written material (and make them more likely to allow investors to keep such material), thus increasing the informational value of such presentations to investors.[143]

Though the proposed reforms should generally increase issuers' ability to use electronic roadshows, the requirement that all free writing be filed with the SEC may dampen issuers' enthusiasm. Even outside the context of the Internet, the proposed filing requirement has produced widespread criticism from securities lawyers who have argued that it would be extremely burdensome to file all free writing material and that the increased liability risks associated with filing would ironically result in a greater shift from written to oral communications than has occurred under the present system.[144] Such

---

140. *See* Reform Release, *supra* note 104, § VII(C), at 81,525 ("[I]ssuers and underwriters could use the Internet and other electronic media to, among other things, conduct electronic roadshows to institutional and retail investors without the use of password protection . . . ."); *New Rules Would End Road Show No-Action Requests, supra* note 139 at 6 (noting that limits on who accessed electronic roadshows would no longer be relevant under the Aircraft Carrier Reform proposal).

141. *See* Reform Release, *supra* note 104, § VII(A)(2), at 81,523 ("Issuers and their agents are known to deliberately provide some information during the waiting period only orally, and also limit the audience to avoid those communications being considered broadcasted. Perhaps the best example of how the current regulatory structure negatively affects investors is the 'road show' structure.").

142. *See* Isaac C. Hunt, Jr., Speech by SEC Commissioner: Navigating the Sea of Communications at the Practicing Law Institute's SEC Speaks (Feb. 26, 1999), *available in* 1999 WL 106714 (S.E.C.), at *3 (arguing that the Aircraft Carrier proposal will bring greater fairness to the market by attacking the "insidious problem of selective disclosure").

143. *See* Reform Release, *supra* note 104, § VII(A)(2), at 81,523-24.

144. *See, e.g.*, Charles Sisk, *Street Ready to Take Shots at SEC Flagship,* CORP. FINANCING WK., Nov. 30, 1998, at 8 ("Most security lawyers say it would be impossible for companies to file all their communications with the SEC, as it would be too difficult to record and track everything."); *"Aircraft Carrier" Sprouts Leaks, supra* note 105 (noting that "companies could just end up concentrating more on oral communications to reduce filings, and

action is especially likely in the context of electronic communications because the Aircraft Carrier Release does not clarify the complicated question of what a "writing" is for the purposes of the filing requirement.[145] Issuers worried about section 12(a)(2) liability for free writings may, therefore, steer wide and clear of anything that could remotely be deemed a writing, making less use of Internet communications than they might otherwise do. Ironically, the SEC seems to acknowledge the difficulty of truly distinguishing oral and written communications in the electronic age by its deregulatory policy toward pre-filing and waiting period communications, but at the same time it is implementing a filing requirement that applies to free *writings*. Electronic roadshows are but one example of the way in which technology has undermined the difference between oral and written communications; the problem can only become more pronounced with the increasing use of multimedia.[146] If the SEC requires issuers to file multimedia presentations, an additional problem is how exactly this should be done given that even the new EDGAR II system will be unable to accommodate multimedia.[147]

Beyond roadshows, the SEC also hopes that the deregulation of communication restrictions during the waiting period will generally allow issuers to make creative use of the Internet and other media technologies to communicate and deliver information to potential investors. The Aircraft Carrier Release notes in particular that issuers would be able to use electronic mail to answer investors' questions about the company and its offering, to engage in "chat room" discussions with investors, and to post messages on bulletin boards about its offering.[148] Again, it is not always clear whether and how these and other materials would be filed with the SEC. For example, would all participants' comments in a chat room discussion need to be filed as free writings, or just the contributions of the company? Could a transcript of a streaming video presentation or a video conference,

---

thus liability.").

145. Section 2(9) of the Securities Act defines a "writing" as a "graphic communication." 15 U.S.C.A. § 77b(a)(9) (West 1997). Securities Act Rule 405 defines a "graphic communication" to include "magnetic impulses or other forms of computer data compilation." 17 C.F.R. § 230.405 (1999).

146. *See* Unger, *supra* note 105, at 33 ("Issuers' growing use of multimedia in traditional written documents and digital information in voice applications has made it difficult for counsel and the Commission staff to determine what is a 'writing' under the Securities Act of 1933.... The problem will multiply as text and multimedia become more intertwined.").

147. *See* Reform Release, *supra* note 104, § VII(B), at 81,525; Unger, *supra* note 105, at 34.

148. *See* Reform Release, *supra* note 104, § VII(C), at 81,525.

neither of which can be recorded, ever provide a fair and accurate representation for other investors? Furthermore, it is not always clear whether filing such information would be of any help to investors. Would, for example, voluminous electronic mail correspondence between a company and potential investors be of any help to other investors?[149]

Another popular use of the Internet that is commonly used by companies to communicate with their investors is corporate web sites. The easing of restrictions on communications is designed to allay at least some concerns regarding liability associated with material posted on or hyperlinked to issuers' web sites. By allowing offers during the pre-filing period, the Aircraft Carrier Release would allow issuers to advertise or provide information about an upcoming offering on their web sites. Thus, issuers would no longer have to worry that something posted on their web site could be interpreted after the fact as a solicitation for an offering.[150] Form A registrants, however, would need to remove any materials not covered by the proposed safe harbors (e.g., "factual business information" and "regularly released forward-looking information") thirty days before filing.[151] By allowing free writings during the waiting period, the Aircraft Carrier Release allows companies conducting an offering of securities to post information relating to the offering on their web site, and to hyperlink to additional relevant information.

Though the easing of restrictions on communications is a positive step, the Aircraft Carrier Release will by no means end concerns over liability stemming from corporate web sites. First, liability is more likely to stem from postings or hyperlinked material being deemed violations of Securities Act section 12(a)(2) or the antifraud provisions than a violation of the section 5 prohibition on communications during the waiting period.[152] Second, the Aircraft Carrier Release may create new difficulties relating to hyperlinks. One reason is the requirement that all free writing material be filed

149. *See* Unger, *supra* note 105, at 34.

150. *See* Allyson Vaughan, *The Offering Quite Period,* FIN. NET NEWS, Oct. 19, 1998, at 8 (noting that "[i]f a firm is communicating with the public during the period of the offering or before the offering, firms must ensure communications are not construed as advertising.").

151. Reform Release, *supra* note 104, § VII(A)(l)(c)(i), at 81,521.

152. *Cf.* Boris Feldman, *Investor Relations on the Internet: A Securities Disclosure Perspective,* OFF-LINE, Winter 1996, at 1, 2, 4 (warning that plaintiffs' lawyers will look on company web sites for forward looking statements that did not come true and for hyperlinks to positive analyst reviews).

with the SEC. Consistency with the "envelope theory"[153] would mean that an issuer would be required to file third party materials if its web site has a hyperlink to such material. If the SEC were to consider imposing such an obligation, it would also have to determine whether such an obligation would be affected by the type of link between the sites, which could vary from a framed link (in which the material from one site is framed by the prior site) to a hyperlink with a prominent exit notice.[154] Hyperlinks also risk running afoul of the requirement that all free writings be accompanied by language instructing investors to read the disclosure documents filed with the SEC.[155] In theory, a company could be liable for failing to provide such language if another site was hyperlinked deep into its web site so as to bypass any cautionary language. Practically, it may also be difficult for a company to file a description of third party free writing material when the company has no control over the content of the third party's web site, which could be changed at any time. Such risks may mean that that issuers will make less use of Internet web sites both to avoid the costs of monitoring numerous web pages and to reduce the risk of liability for filed free writings under section 12(a)(2) of the Securities Act.[156]

The Aircraft Carrier Release's prospectus delivery proposals may also affect Internet usage. However, the new approach should merely shift, but not reduce, the difficulties involved in electronic dissemination of required information. On the one hand, the elimination of the requirement that a final prospectus be delivered before sale makes the many difficulties involved in meeting the notice, access, and delivery criteria irrelevant. The Aircraft Carrier Release requires only that an issuer inform investors of where they can obtain the information that constitutes the final prospectus free of charge.[157] A note sent along with the term sheet (in the case of Form B issuers) or presumably with either the preliminary prospectus or even the confirmation letter (in the case of Form A issuers) telling investors that the final prospectus is available on the issuer's and/or the SEC's web site would be sufficient to meet this requirement.[158] On the other hand, the requirement that investors be provided with a

153. *See supra* note 77 and accompanying text.

154. *See* Unger, *supra* note 105, at 33.

155. *See* Reform Release, *supra* note 104, § VII(A)(2), at 81,524.

156. *See SIA Opposes Aircraft Carrier Filing Requirements*, FIN. NET NEWS, Mar. 1, 1999, at 7.

157. *See* Reform Release, *supra* note 104, § VIII(C)(3)(a), at 81,536.

158. *See id.* § VIII(C)(3)(a) n.395.

term sheet or preliminary prospectus before the investment decision is made would seem to raise all the notice, access, and delivery concerns that currently apply to the final prospectus. Furthermore, current Exchange Act Rule 15c2-8, which mandates that broker-dealers deliver a final prospectus to investors forty-eight hours before sale in the case of an initial public offering, notably does not apply to issuers.[159] Therefore, in a direct public offering conducted over the Internet (which by definition would not utilize a broker-dealer), the prospectus need only be delivered upon sale, creating a unique benefit to Internet-based direct public offerings in the current system.[160] However, the Aircraft Carrier Release Provisions involving the term sheet and preliminary prospectus explicitly apply to issuers as well as broker-dealers, thereby creating the same delivery requirements for direct public offerings and all other offerings.

III. CONCLUSION

The combination of substantial cost savings and an unprecedented ability to reach millions of investors means that issuers have strong incentives to utilize the Internet to raise capital. Fear of liability, however, can easily stifle innovation in this area. Though the SEC has so-far embraced new technologies, such as EDGAR, the current regulatory regime still assumes a paper-based world. Where it does not, the laws draw paper-based analogies: the *envelope* theory; the requirement of substantial equivalence between electronic and paper delivery; and the proposal that free *writings* be filed. With the increasing use and complexity of multimedia communications, the SEC will continually need to revisit its assumptions. The Aircraft Carrier Release reveals the SEC's ability to do so. However, while the current approach to reform does aid issuers who use new technologies in important ways, this paper has also shown that some serious pitfalls remain for those involved in securities offerings conducted over the Internet.

The SEC could further promote the use of the Internet in securities offerings in two specific ways. First, the SEC should provide official guidance, either in the form of a release or regulations, to issuers conducting securities offerings over the Internet that are exempt from the registration requirements. Companies wishing to raise small sums over the Internet, or services linking such issuers with investors, should no longer have to rely on a string of

159. *See* Exchange Act Rules, 17 C.F.R. § 240.15c2-8 (1999).

160. *See* Reform Release, *supra* note 104, § VIII(C)(1), at 81,535.

no-action letters to guide their actions. Indeed, the president of IPONet has complained that most companies have refused to use his service due to fear of liability, despite the fact that IPONet itself was granted a no-action letter.[161]

Second, the SEC should eliminate the proposed requirement that free writings disseminated during the pre-filing or waiting periods be filed with the SEC. This requirement could undermine many of the provisions, especially those relating to pre-filing and waiting period communications, that would otherwise promote the use of the Internet. The requirement is also unnecessary: when information is made publicly available on the Internet (for example by posting it on a company's own web site), there is no need for the same information to be filed with the SEC, who would merely post this information on its own web site. This is not to say that no investor protection is needed, but perhaps there are other possibilities, such as a requirement that such material remain on an issuer's web site for the duration of an offering. In addition, the antifraud provisions would still apply to all such material, whether filed or not. Thus, eliminating the filing requirement could potentially go a long way toward helping to integrate the Internet and its many possibilities into the securities offering process.

161. *See* Reinbach, *supra* note 3, at 40. Leo Feldman, the company's president, explained why 20 companies to whom he had talked about participating in IPOs turned him down.

> Their biggest fears are that something might be released by e-mails or something else that would [prompt the Securities and Exchange Commission (SEC) to] step in and say they were gun-jumping or something .... It's been like pulling teeth .... Everybody is afraid. The underwriter's counsel are afraid, even though I have a No Action letter from the SEC [stating that it will not interfere with IPO.Net's Web IPOs]; they don't think I can do this. When you talk to counsel of the issuer, you run into trouble, and [the same] when you start talking to counsel of the broker-dealer. Nobody wants to opine to the fact that this is legal.

Id.

Pirates of the 21st Century: The Threat and Promise of Digital Audio Technology on the Internet

Rebecca J. Hill[†]

> [A]s sure as you or I are sitting in this courtroom today, some bright young entrepreneur . . . is going to come up with a device to unjam the jam. And then we have a device to jam the unjamming of the jam and we all end up like jelly.[1]

TABLE OF CONTENTS

[†] Articles Editor, Santa Clara Computer and High Technology Law Journal, Vol. 16. J.D. candidate, Santa Clara University School of Law, 2000; B.S. University of Colorado, Boulder. E-mail hillrj@bigfoot.com. The author gratefully acknowledges Ryan Hilbert, Jennifer Ishimoto, Brennan Peterson, Professor Thomas Schatzel, and Jennifer Burke Sylva whose meaningful comments on earlier drafts of this article contributed much to its final form. Additional thanks is due to the entire board of editors of Vol. 16 for their support and patience, and especially to my technical editor, Barrett Schaefer and the Vol. 17 candidates for their cite-checking assistance in preparing this comment for publication.

The author and the Journal acknowledge that due to the transient nature of the Internet, certain web sites may no longer be active after this article is published. Hence, web site references are on file with the Santa Clara Computer and High Technology Journal.

1. PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: THE LAW AND LORE OF COPYRIGHT FROM GUTENBERG TO THE CELESTIAL JUKEBOX 159 (1994) [hereinafter GOLDSTEIN] (citing JAMES LARDNER, FAST FORWARD, 119-20 (1987) (reporting on Judge Ferguson's observations during the *Sony* trial). When one of the plaintiffs in the *Sony* trial offered expert testimony that a "low cost jamming device" could make it impossible to "record a television program without the copyright owner's permission," it is reported that Judge Ferguson's reaction was pointed as to what would happen if he were to order Sony to put such a jamming device in its video recorders. *See id.*; *see also* Universal Studios, Inc. v. Sony Corp. of Am., 480 F. Supp. 429 (C.D. Cal. 1979).

I. INTRODUCTION

The Internet is changing the way many organizations conduct business. The recording industry is one such example. Digital music technologies and the Internet now allow for the promotion, distribution, broadcast, and sale of music on-line every day.[2] A March 1999 Forrestor study predicts that sales of downloadable music through the Internet will reach $1.3 billion by 2003.[3]

One of the leading agents of this revolution is a popular digital audio compression technology called MP3.[4] MP3 technology permits extremely high-quality audio to be "transferred, stored, and categorized on almost any computer."[5] In the past three years, students at college campuses equipped with high-speed networks have been utilizing MP3 to "rip CD tracks and trade them" on the Internet.[6]

---

2. *See* Jeffrey D. Neuburger & Susan Israel, *Music Industry Acts in Concert on Sound Samples: Harmonious Compromise Could Resolve Licensing Issues Arising From the Downloading of Music*, NAT'L L.J., Jan. 26, 1998, at C17.

3. *See* James Ledbetter, *The Size Problem*, THE INDUS. STANDARD, Feb. 7, 2000, at 61 (stating that the $1.3 billion figure "overlooks the paradox intrinsic to the idea of major labels running the digital download business: if they start charging, they will remove a major part of its appeal; if they keep it free, they cannibalize their own sales."); *see also* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1074 (9th Cir. 1999) (citing Jupiter Communications, *Jupiter Projects Meager $30m in Digital Distribution Revenue*, July 15, 1998 (press release), *available in* 1998 WL 14096262 (that on-line sales in pre-recorded music will exceed $1.4 billion by 2002 in the United States)).

4. MP3, which stands for "Motion Picture Experts Group-1 audio layer three," is the most popular form of digital audio compression available on the Internet. For more information about MP3 audio compression, *see* KIERSTEN CONNER-SAX & ED KROL, THE WHOLE INTERNET: THE NEXT GENERATION 360 (1999).

5. CONNER-SAX & KROL, *supra* note 4, at 360.

6. Randall Rothenberg, *Rob Glaser, Moving Target: The Man Behind the RealPlayer Races Ahead with RealJukeBox, His Aggressive Scheme to Dominate the Downloadable Universe*, WIRED, Aug. 1993, at 126, 132. "Ripping" is the term used to describe the process of taking music from a CD and converting it to MP3 format. *See* CONNER-SAX & KROL, *supra*

Similarly, MP3's popularity has invigorated numerous entrepreneurs, music fans, and musicians to design innovative MP3 peripherals.[7] Several factors contribute to MP3's impact, most notably: (1) the affordability of computers, most equipped with CD-ROM and sound output; (2) the growth of the Internet and its host of decentralized e-commerce possibilities; and (3) the promise of broadband, high-speed Internet access to consumers.[8]

The excitement about the Internet and digital audio technology has been accompanied by trepidation from the established recording industry. More specifically, the recording industry, "accustomed to having solid control over product distribution," is especially concerned by the way the Internet is changing traditional models of music distribution and transmission.[9] Since 1994, The Recording Industry Association of America (RIAA),[10] a lobbying group representing record companies, has been very concerned about its ability to enforce its copyrights in light of the ease in which "sound recordings and other information" may be uploaded and distributed.[11]

---

note 4, at 363 ("Programs called CD 'rippers' take tracks played by your computer's CD-ROM drive and store them in electronic form on your hard drive. The resulting files can be encoded as MP3.").

7. For example, several MP3 players are in development, including portables, home stereo components, and car stereos. *See* Jesse Freund, *The MP3 Players*, WIRED, Aug. 1999, at 136-137.

8. CONNER-SAX & KROL, *supra* note 4, at 361; *see also* Christopher Jones, *Digital Music at the Crossroads* (Apr. 19, 1999) <http://www.wired.com/news/culture/0,1284,19171,00.html> (quoting Marc Geiger, CEO of Internet music company "Artist Direct": "In the next five years, you'll start to see higher-bandwidth connections, and as that happens, you'll see a shift in the economy of the music business.... We'll need to figure out other revenue streams to make up for this loss of value. In the short term, it's going to be a nightmare.").

9. *See* Beth Lipton Krigel, *Music Firms Mull Net Copyright Claim* (June 15, 1998) <http://www.news.com/News/Item/0,4,23170,00.html> (reporting on the dilemma facing the recording industry: "On one hand, [the industry] wants to be active on the Net, where analysts say billions of dollars will change hands for music in the next five years. At the same time, however, the industry is fighting for control of a global medium ...."); *see also* Alan Saracevic, *A Wrench in the Music Machine On-line Migration is Changing the Face of the Recording Industry*, S.F. EXAMINER, Dec. 20, 1998, at B1 (stating that the music industry is "fearing the Internet's potential for piracy").

10. The RIAA represents nearly all of the record companies in the United States. *See generally About Us: Frequently Asked Questions about the RIAA* (visited Mar. 10, 2000) <http://www.riaa.com/about/ab_faq.htm>; *see also About Us* (visited Mar. 10, 2000) <http://www.riaa.com/about/aboutus.htm> ("Our mission is to foster a business and legal climate that supports and promotes our members' creative and financial vitality around the world. In support of our mission, we work to protect intellectual property rights worldwide and the First Amendment rights of artists; conduct consumer, industry and technical research; and monitor, review and influence state federal laws, regulations and policies.").

11. *See* Russell Shaw, *CES – Recording Industry Exec Calls Internet "Threat,"*

As a result of these concerns, the RIAA and individual record companies have been aggressive about enforcing their intellectual property rights on-line.[12] The resulting controversy surrounding MP3 and new MP3-based services and technologies has generated tremendous discussions regarding intellectual property, the Internet, and the music industry.[13]

This comment will address some of the issues raised by MP3-related litigation and examine the difficulties in balancing the interests mentioned above.[14] To this end, Part II will provide some background information about the Internet and privacy concerns raised by digital audio technology. Part II will also include an introduction to provisions in U.S. copyright law that govern musical works and discuss the scope and limitations of a copyright owner's exclusive rights to reproduce and distribute his or her works in conjunction with both the Internet and digital audio technologies.

Following this discussion, Part III will then explore the impact that MP3 technology and digital music on the Internet may have on the recording industry and will provide some background information on recent cases that expose the complex web of interests including copyright law, digital audio technology, and the Internet. Next, Part

---

NEWSBYTES NEWS NETWORK, June 23, 1994, *available in* 1994 WL 2416354 (quoting RIAA's David Leibowitz saying the RIAA "says it is concerned about the specter of bulletin board system (BBS) owners digitizing a CD, capturing it in computer memory, and then sending it out over the BBS to anyone with Internet access who chooses to receive the material."); *see also* Laurent Belsie, *Who Pays for What on Tomorrow's Internet?*, CHRISTIAN SCI. MONITOR, Oct. 25, 1995, at 1, *available in* 1995 WL 6397558 (stating that "many Internet experts argue that this technology soon will overwhelm the copyright laws.").

12. *See* Andrew Leonard, *Mutiny on the Net* (visited Mar. 5, 2000) <http://www.salon.com/21st/feature/1998/03/cov_20feature.html>.

13. MP3 and copyright law on the Internet underscore "a number of issues regarding copyright and intellectual property law that have pitted record industry stalwarts against underground music distributors." Jim Hu, *Music Group Sues Over MP3 Device* (Oct. 9, 1998) <http://www.news.com/News/Item/0,4,27376,00.html>. Problems and opportunities associated with digital musical distribution are illustrative of many of the issues intellectual property rights owners will face as the Internet matures. *See* Ross J. Charap & Jessica L. Rothstein, *O'er the Ramparts We Watched: The Struggle to Control the Distribution of Music on the Internet*, INTELL. PROP. TODAY, Sept. 1999, at 18, *available in* LEXIS, Legal Publications Group File ("[T]he Internet has been called 'the world's largest copying machine.' Nowhere are these problems more evident than in the recording industry where music's digital tribulations illustrate many of the issues intellectual property owners face as the Internet matures."). *See also Electronic Frontier Foundation Digital Audio and Free Expression Policy Statement* (May 1999) <http://www.eff.org/cafe/eff_audio_statement.html> (stating it is not just about music: "All kinds of information flows in digital audio forms, including talk radio, political speeches, commercial speech . . . public meetings and speeches . . . and spoken books.").

14. These interests are representative of the public and private interests inherent in United States copyright law. *See* discussion *infra* Part II.C.

IV will present critical observations regarding some of the proposals that have been offered by the recording industry and other interested parties for "securing" copyrighted audio content.

Ultimately, in Part V, this comment concludes that just as targeting the "players" for contributory copyright infringement has failed in the past,[15] the RIAA and other copyright owners will probably not significantly deter business and consumer interest in digital audio technology by advocating radical changes in copyright law. Although the Internet presents new complexities, it does not change the nature and underlying purpose of copyright law. While unauthorized reproduction of copyrighted works is a valid concern for the recording industry, any measures to curb piracy must also consider the public interest in addition to the limitations on the copyright monopoly—legitimate non-infringing uses of digital audio technologies, like MP3. The Internet is providing new ways for many businesses to provide services and generate income. The recording industry must not force changes in the law that stifle this growth, but instead should adjust its own business practices to conform in a lawful manner.

II. BACKGROUND

A. The Internet and Digital Audio Technology

The Internet is a two-decade old global network of interconnected computers proven to have a substantial impact on everyday life.[16] Many different programs use the Internet, perhaps most notably electronic mail, newsgroups, and the World Wide Web

15. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984).

16. *See* Reno v. ACLU, 521 U.S. 844, 849 (1997); *see also* Barry M. Leiner et al., *A Brief History of the Internet* (visited Mar. 5, 2000) <http://www.isoc.org/internet/history/brief.html> [hereinafter *ISOC*]. The Federal Networking Council (FNC) passed a resolution defining the term 'Internet' in October of 1995. Developed "in consultation with the leadership of the Internet and Intellectual Property Rights (IPR) Communities," the resolution defines "Internet" as

> the global information system that—(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

Federal Networking Council, *FNC Resolution: Definition of "Internet"* (Oct. 24, 1995) <http://www.fnc.gov/Internet_res.html>.

(the "Web").[17] Such programs can be used to transmit and receive audio and video content over the Internet.[18] According to one of the inventors of the Web, "[t]he Web made the Net useful because people are really interested in information (not to mention knowledge and wisdom!) and don't really want to have to know about computers and cables."[19] In short, the Internet has developed into more than just a collection of technologies, it is a collection of communities.[20]

An enthusiastic community has grown around MP3 since 56K modems and 300+ MHZ Pentium processors became standard on PCs.[21] Compressing audio files to about one tenth of their original size, MP3 technology allows digital audio files to be transferred "more quickly and stored more efficiently . . . without significantly reducing sound quality."[22] Coupled with the rise of broadband Internet access—such as cable modems and DSL—MP3 provides an individual the ability to download an hour of music to a personal computer in a fraction of that time.[23] The popularity of MP3 is fueled by the format's freely available, non-proprietary compression technology, and the array of peripherals that incorporate MP3 technology.[24] By adopting the MP3 standard, a number of technologies and services have emerged that allow consumers, hardware manufacturers, retailers, artists, and record companies to

17. These three programs were discussed in Reno v. ACLU, 521 U.S. 844 (1997).

18. *See id.* at 851.

19. Tim Berners-Lee, *Frequently Asked Questions by the Press* (visited Mar. 10, 2000) <http://www.w3.org/People/Berners-Lee/FAQ.html>. Tim Berners-Lee conceived of the Web in 1989 and leads the World Wide Web Consortium (W3C), an organization responsible for coordinating the evolving standards associated with the Web.

20. *See ISOC*, *supra* note 16.

21. *See* Michael Behar, *It's Playback Time! And MP3 Is Only the Beginning*, WIRED, Aug. 1999, at 122.

22. Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1074 (9th Cir. 1999); *see also* CONNER-SAX & KROL, *supra* note 4, at 360-61 (explaining that MP3s "[turn] raw sound data . . . into compressed representation via a set of complex mathematical transformations . . ." and providing the following example: "A five minute song at standard CD quality expressed as raw data is: 44,100 (sampling rate)*2 (bytes per sample)*2 (channels)*60*5=52,920,000 bytes, while a five-minute song compressed with MP3 with the usual encoding options is only: 128,000 (Kbps encoding rate, 2 channel)/8 bits per byte*60*5=4,800,000 bytes."). *Id.*

23. *See* Vincent J. Roccia, Comment, *What's Fair is (Not Always) Fair on the Internet*, 29 RUTGERS L.J. 155, 161-62 (1997) (noting that compression facilitates the reproduction of large quantities of copyrighted material that can be disseminated through the global computer network in a matter of seconds).

24. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d at 1074 (suggesting that the "freeness" of MP3 makes it preferable to other proprietary technologies); *see also* Freund, *supra* note 7.

utilize advanced digital audio features.[25]

B. The Players

Whether downloaded from the Internet or "ripped" from a consumer's compact disc ("CD") collection, acquiring and listening to MP3 files is easy. Thousands of songs in the MP3 format—some authorized by performers, others not—may be downloaded from the Web at the click of a button.[26] In fact, "MP3" is one of the most frequently searched terms,[27] and many search engines have a feature allowing MP3-specific searches.[28] To help artists and record companies promote their products, and to assist music fans in sorting through the multitudes of MP3s, several MP3-specific "portals" have opened on the Web.[29] After locating a desired song, the MP3 version of the song can be downloaded onto a computer. Consequently, a user can then use a "decoder" program to play the file through their computer's soundcard or upload it to a portable MP3 player.[30]

---

25. *See* Ted Greenwald & Michael Behar, *Follow the Music: The Etune is Going Places*, WIRED, Aug. 1999, at 124-25.

26. Of those authorized, some are free. However, other artists require a fee for downloading their works. *See Rykodisc Endorses MP3* (Feb. 4, 1999) <http://www.wired.com/news/news/technology/story/17727.html> (reporting that Rykodisc is the largest music label to endorse MP3 digital audio format and conveying that Rykodisc's decision to sell in that format was a "simple recognition of reality: MP3 is here, it's being used, and to ignore it would only lead to more music pirating."). The music industry also recognizes the potential for revenue from using the Internet to deliver music. *See Testimony Before the House Commerce Comm., Subcomm. on Telecommunications, Trade and Consumer Protection* (Oct. 28, 1999) (statement of Hilary Rosen, President & CEO, Recording Industry Association of America) <http://www.riaa.com/musicleg/press/102899.htm> [hereinafter *Testimony of Hilary Rosen*].

27. Internet search engines www.Searchterms.com and Lycos.com both claim the term "MP3" is the second most frequently searched term, after "sex." *See* Ronald Warren Deutsh, *Lycos Gets Fast with MP3* (Feb. 1, 1999) <http://www.wired.com/news/news/culture/story/17651.html>.

28. For example, the search engine Altavista.com offers MP3-specific searches. While such search capabilities can be helpful, frustration often ensues because many links lead to discontinued pirate music sites which have been shut down by the RIAA. *See generally* Georgie Raik-Allen, *Players Line Up For Battle Over Online Music Industry* (Feb. 2, 1999) <http://www.redherring.com/insider/1999/0202/news-music.html>; *see also* Michael Robertson, *Shutting Down Pirates in 4 Easy Steps* (Nov. 30, 1998) <http://www.mp3.com/news/119.html> (noting "[a]s easy as it is for the pirate to find songs, it's equally easy to find for policing purposes. The quickest way is to use one of the many search engines which have the ability to locate MP3 files specifically.").

29. *See, e.g., About MP3.com* (visited Feb. 6, 2000) <http://www.mp3.com/aboutus.html> ("MP3.com is the premier Music Service Provider (MSP) allowing consumers to instantly discover, purchase, listen to, store and organize their music collection from anywhere, at any time, using any Internet device.").

30. CONNER-SAX & KROL, *supra* note 4, at 362-63.

Alternately, using a computer equipped with a CD-ROM, an MP3 encoder,[31] and a CD collection, a user can store his or her favorite songs on a computer hard drive. Once the music from the CD is converted into the MP3 format, it can easily be distributed among users in the same way as any other computer file—via a web page, an FTP site, on a disk, as an e-mail attachment, etc.[32]

Numerous new products have been introduced that offer music fans a range of extended services that take advantage of MP3's compressed, digital format. Three specific technologies and services (and the controversy surrounding them), will be discussed in this comment: (1) The Rio portable MP3 player; (2) Napster; and (3) My.MP3.com.[33]

The first product, the *Rio* PMP300 (the "Rio") portable music player is the most established technology that supports the popular MP3 format.[34] Introduced in November 1998, by Diamond Multimedia Systems, Inc., the Rio is a computer peripheral designed specifically for digital audio in the MP3 format. MP3 files stored on a computer hard drive are uploaded to the Rio. The Rio, having no moving parts, is capable of playing back MP3 files without any of the skipping traditionally present in portable CD players.[35] After overcoming legal barriers,[36] the Rio has garnered favorable consumer reviews, and other companies are developing similar and competing

---

31. An MP3 encoder is a software program that converts the digital embodiment of the music from the CD using MP3 compression. Many programs are available as freeware or shareware on the Internet. *See id.* at 363.

32. *See id.* at 361.

33. For a discussion of the legal issues, see discussion *infra* Part III.A.

34. *See Diamond Multimedia Ships Industry's First Widely Available Portable Internet Music Player, The Rio PMP300* (Nov. 23, 1998) <http://www.diamondmm.com/companypress_centerpress_releases.asp?ID=232> (press release) [hereinafter *Diamond Press Release*].

35. *See id.*

> The *Rio* PMP300 is smaller than an audio cassette and has no moving parts so it won't skip, even during extreme movement. It is powered by a single AA alkaline battery for up to 12 hours of continuous playback. 32 MB of onboard flash memory provides up to 60 minutes of continuous digital quality playback and up to eight hours of voice quality audio. An add-on flash memory upgrade card is also available in a half-hour (16MB) configuration for $49.95 (ERP) and a one-hour configuration (32MB) will be available in February for an ERP of $99.95.

Id. See also Rio PMP 300 Key Features (visited Mar. 10, 2000) <http://209.10.46.178/default.asp?menu=RIO_300&sub_menu=>.

36. See discussion *infra* Part III.A.1. for a description of the legal activities surrounding the *Rio* player.

players, including an MP3 player for use in automobiles.[37] The playback possibilities, including emergence of CD players that can simultaneously decode and play MP3 files have helped establish MP3 as the de facto standard in audio compression.[38]

Second, a downloadable software program called Napster allows users to swap MP3 audio files directly from their computers.[39] Although still in its "beta" release, the Napster program has spread quickly, prompting some to describe its user base as "the fastest growing community in the history of the Net. . . ."[40] Napster users store MP3 files on their hard drives and the Napster program sends a list of the songs on a user's hard drive to its central servers, thereby creating a giant searchable MP3 database.[41] With Napster, users can locate and download their favorite music (in the MP3 format) with a "convenient, easy-to-use interface."[42] The future of Napster is uncertain. In December 1999, the RIAA filed a federal lawsuit against

---

37. *See* Theta Pavis, *Taking MP3 to the Streets* (Feb. 4, 1999) <http://wired.com/news/news/culture/story/17720.html> (reporting that the surge in popularity of the MP3 format has driven "an informal network of people" to develop MP3 car-players). *See also* CONNER-SAX & KROL, *supra* note 4, at 364; *See* Freund, *supra* note 7, at 136.

38. *See generally* Charap & Rothstein, *supra* note 13; *see also* Pavis, *supra* note 37 (reporting the announcement that Internet music label GoodNoise and computer peripheral designer Adaptec have teamed up to develop software that will let CD players and car stereos read MP3 files recorded on CDs).

39. Courtney Macavinta, *Schools Crack Down on Net Music Software Napster* (Jan. 20, 2000) <http://news.cnet.com/category/0-1005-200-1527930.html>; *see also* Janelle Brown, *MP3 Free-For-All* (Feb. 3, 2000) <http://www.salon.com/tech/feature/2000/02/03/napster/index.html> (stating that Napster lets music fans "turn their computers into servers for the purpose of swapping MP3 files.").

40. Brown, *supra* note 39.

41. Unlike My.MP3.com, Napster does not store music on its own central servers; Napster merely facilitates the union of "downloader and downloadee." *Id.*

42. *So, What the Heck is Napster?* (visited Mar. 5, 2000) <http://www.napster.com/whatisnapster.html>. This web site includes the following description:

> Napster is a completely new way of thinking about music online. Imagine. . .an application that takes the hassle out of searching for MP3s. No more broken links, no more slow downloads, and no more busy, disorganized FTP sites. With Napster, you can locate and download your favorite music in MP3 format from one convenient, easy-to-use interface.
>
> What else does it do? Quite a bit, actually. Some highlights include:
>
> PRIVATE CHAT – Allows Users to chat with each other in forums based on music genre.
>
> AUDIO PLAYER – Plays MP3 files from right inside Napster, in case your don't have an external player or would prefer not to use one.
>
> HOTLIST – Lets your keep track of your favorite MP3 libraries for later browsing.

Id.

Napster in California alleging contributory and vicarious copyright infringement.[43]

Finally, "My.MP3.com," a "virtual CD player" service recently introduced by MP3.com, allows consumers to access the music they own on CD from any computer connected to the Internet.[44] MP3.com boasts an advanced set of security features—ownership is verified either through a digital receipt provided when a CD is purchased through a MP3.com retail partner, or through MP3.com's "Beam-it" software program—and claims that the only way to "get music into a My.MP3.com account is to own a physical CD."[45] To understand this service better, consider the following example. After placing a CD in a CD-ROM drive, Beam-it loads the music into an My.MP3.com account in a matter of seconds and verifies ownership by locating and uploading a code embedded from the CD to MP3.com. Subsequently, a user can then log onto their password-protected account and hear any song from their CD collection from any place with an Internet connection.[46] Like Napster, My.MP3.com has been met with some resistance. In January 2000, the RIAA filed a federal copyright suit in New York against MP3.com alleging that its My.MP3.com service violates the exclusive rights to reproduce copyrighted sound recordings.[47]

The fidelity, compressibility, and transferability of the digital form make it all but "irresistible" when compared to the alternatives of analog recordings.[48] The digital format and its provision of "accessibility to the power of the modern digital computer," is

43. *See Ground Zero: The Future of Digital Music* (visited Mar. 5, 2000) <http://www.napster.com/groundzero>; *see also Recording Industry Sues Napster for Copyright Infringement* (Dec. 12, 1999) <http://www.riaa.com/piracy/pir_pr.htm>.

44. *See My.MP3.com Questions & Answers* (Jan. 20, 2000) <http://bboard.mp3.com/mp3/ubb/Forum8/HTML/000050.html>. This web site exists to help explain the "new and improved My.MP3.com" and to answer some common questions about the program. At one point, it is explained that "because the music is stored on the Net, a music fan can listen to their music library from work, home or any location which has a computer with Net access. Since more and more places are getting computers (e.g. some health clubs now have Net-enabled computers), this allows you to take your music with you." *Id.*

45. *Id.*

46. *See* Eliot Van Buskirk, *Music Distribution Evolves Another Step* (visited Mar. 14, 2000) <http://www.cnet.com/consumerelectronics/0-3622-7-1542301.html?st.ce.3622-7-1542300.txt.3622-7-1542300>.

47. *See Compl. for Copyright Infringement*, UMG Recordings, Inc., et al. v. MP3.com, Inc. (S.D.N.Y. 2000) (No. 00 Civ. 0472), *available at* (visited Mar. 16, 2000) <http://www.mp3.com/news/533.html>.

48. *See* GOLDSTEIN, *supra* note 1, at 197-99. In addition, the "clarity and durability" of the digital form "far exceeds" analog alternatives. *Id.*

integral to the thriving digital environment, the "new communications infrastructure."[49] The recording industry and some copyright owners fear that consumers will stop purchasing pre-recorded music (records, tapes, and CDs), if consumers can easily download music from the Internet. This fear includes not only the loss of revenue attributable to pirated music, but perhaps more significantly, the loss of a familiar way of doing business.[50] Thus, the MP3 format has the music industry wondering what copyright law can do to protect its valued intellectual property.[51]

C. United States Copyright Law

Copyright is generally regarded as intellectual property.[52] The intellectual component of copyright is the "products of the human mind,"[53] which is "incapable of possession except as it is embodied in a tangible article,"[54] such as a song recorded on a CD or lyrics in print. Copyright, like other forms of property is vulnerable to theft. Copyright owners rely upon copyright laws and lawyers to defend their musical works against piracy.[55]

Copyright law originates from Article I, Section 8, Clause 8 of the United States Constitution.[56] The Constitution grants Congress the power to confer limited exclusive rights upon authors and inventors "to promote the Progress of Science and the useful Arts."[57] At the "heart" of copyright law is a delicate balance between public and private interests; however, it is not always easy to determine which is which.[58] The theory is that copyright protection benefits

---

49. *Id.* at 198.

50. *See* CONNER-SAX & KROL, *supra* note 4, at 362; *see also* Vito Peraino, *The Law of Increasing Returns, Memo to the Music Industry: It's time to listen to the sound of the future*, WIRED, Aug. 1999, at 144.

51. *See* Daniel W. McDonald et al., *Intellectual Property and the Internet*, THE COMPUTER LAW., Dec. 1996, at 8 (emphasizing the host of legal issues, including copyright infringement, arising due to the ease of "accessing, reproducing, and transmitting digitized information").

52. *See* ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT CASES AND MATERIALS 12 (5th ed. 1999).

53. GOLDSTEIN, *supra* note 1, at 9.

54. GORMAN & GINSBURG, *supra* note 52, at 12.

55. *See* GOLDSTEIN, *supra* note 1, at 8-9; *see also*, BLACK'S LAW DICTIONARY 1148 (6th ed. 1990) ("Piracy. Those acts of robbery and depredation upon the high seas which, if committed on land, would have amounted to a felony .... The term also applied to the illegal ... reproduction of copyrighted matter ....").

56. U.S. CONST. art. 1, § 8, cl. 8.

57. *Id.*

58. *See* GOLDSTEIN, *supra* note 1, at 12-14.

society when the system of exclusive rights stimulates the dissemination of creative works.[59] The public receives the benefits of a wide range of creative expression while financial and social rewards encourage continued ingenuity and productivity.[60] However, this is a fragile balance. Congress has been granted the task of

> defining the scope of the limited monopoly that should be granted to [creators] in order to give the public appropriate access to their work product. Because this task involves a difficult balance between the interest of authors and inventors in the control and exploitation of the writings and discoveries on the one hand, and society's competing interest in the free flow of ideas, information, and commerce on the other hand, our patent and copyright statutes have been amended repeatedly . . .[61]

Congress codified this attempt to balance promoting creative expression with society's interest in access to the products of that expression in the Copyright Act of 1976.[62] The Copyright Act grants to authors of "original works of authorship" certain exclusive rights, including the right to: reproduce such works; to prepare derivative works; to distribute copies or phonorecords; to perform or display the works publicly; and to perform sound recordings publicly by means of a digital audio transmission.[63] The Act describes the duration, subject matter, scope, causes of action, and limitations to those exclusive rights.[64]

1. Copyright And Musical Works

Most musical works involve two distinct copyrighted works: (1) the underlying musical composition (*e.g.* musical notation and lyrics); and (2) a physical embodiment of a particular performance of that musical composition, usually in the form of and referred to as a "sound recording."[65] While musical works on the Internet often

---

59. *See* GORMAN & GINSBURG, *supra* note 52, at 14 (noting that ".the interest of authors must yield to the public welfare where they conflict . . .").

60. *Id.* at 14.

61. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984).

62. Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended at 17 U.S.C. §§ 101-1332 (1994)).

63. 17 U.S.C. § 106 (1994). Although these rights are often intertwined, this comment focuses primarily on the reproduction rights—the right to make copies.

64. *Id.* §§ 101-121.

65. 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT §§ 2.05[B], 2.10 (1999) [hereinafter NIMMER]. Until 1972, no federal copyright protection was available for sound recordings. Lewis Kurlantzick & Jacqueline E. Pennino, *The Audio Home Recording Act of 1992 and the Formation of Copyright Policy*, 45 J. COPYRIGHT SOC'Y U.S.A. 497, 499

implicate copyright claims in both the musical composition and the sound recording, this comment will focus on the sound recording, rather than the composition.[66] Generally, each of the copyrighted works has a different owner. For example, the composer of a work, or the composer's publisher, usually owns the copyright in the composition, while a record company typically owns the copyright in the sound recording.[67] The sound recording is usually the subject of an overall contractual relationship between the performer and his or her record company.[68] Most business relating to musical works concerns itself with the production, sale, and distribution of recorded music.[69] The recorded embodiment and the exclusive rights of reproduction and distribution of a musical work are more directly implicated in the controversy surrounding MP3.

2. Limits to the Exclusive Right to Reproduce—Fair Use Doctrine, *Sony*, and the AHRA

Attempts to address music piracy and the rights of consumers regarding digital music on the Internet are evident in existing limitations embodied in the Copyright Act and the history of copyright law and new media. The fair use doctrine, codified in § 107 of the Copyright Act, is one example of how Congress has addressed the tension between the public and copyright owners, by limiting the exclusive rights of the latter.[70] The doctrine was originally created by the courts and allows a third party to "use the copyrighted material in a reasonable manner without consent, notwithstanding the monopoly granted to the [copyright] owner."[71] The doctrine also provides an affirmative defense to copyright infringement and requires courts to avoid the rigid application of the copyright statute when it would stifle the very creativity that the law

(1998).

66. Note, however, that the two components often travel together. *See* GORMAN & GINSBURG, *supra* note 52, at 514.

67. *See* NIMMER, *supra* note 65, § 8.19[A]. Licensing to cover performance rights—the contributions by the composers and publishers for the underlying composition—are generally handled by performance rights societies, BMI or ASCAP, while the mechanical reproduction of the composition is generally handled by the Harry Fox Agency. *See id.*

68. *Id.* § 24.01.

69. *See id.*

70. 17 U.S.C § 107 (1994).

71. Rosemont Enters., Inc. v. Random House, Inc., 366 F.2d 303, 306 (2d Cir. 1966), *cert. denied*, 385 U.S. 1009 (1967) (citing H. BALL, COPYRIGHT AND LITERARY PROPERTY 260 (1944)).

is designed to foster.[72]

Courts have recognized that the fair use doctrine strikes a balance between the dual risks created by the copyright system; namely, that although depriving authors of their monopoly may reduce their incentive to create, granting authors a complete monopoly could reduce the creative ability of others. Because the fair use doctrine gives courts some flexibility in applying copyright law, the fair use doctrine will probably play a pivotal role in the development of copyright law on the Internet.

One of the foremost cases dealing with fair use is *Sony Corp. of America v. Universal City Studios.*[73] In *Sony*, plaintiffs Universal City Studios and Walt Disney Co. alleged that defendant Sony Corporation, the manufacturer of the Betamax videocassette recorder, was liable for contributory copyright infringement and that the home taping of copyrighted television programs for later viewing (a practice the court dubbed "time-shifting") violated Universal and Disney's copyright in those programs.[74] Defendant Sony asserted the fair use doctrine as an affirmative defense. Ultimately, the Supreme Court held that the act of home video taping for private viewing constituted fair use and was thus non-infringing.[75] Justice Stevens embodied this conviction when he delivered the Court's ultimate ruling: "[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses."[76] Thus, the Supreme Court concurred with the District Court's assertion that, "[W]hatever the future percentage of legal versus illegal home-use recording might be, an injunction which seeks to deprive the public of the very tool or article of commerce capable of some noninfringing use would be an extremely harsh remedy, as well as one unprecedented in copyright law."[77]

Following the Court's decision in *Sony* and in response to the introduction of a new private copying medium called digital audio tape (DAT), artists and music producers alike feared that the new ability to make perfect copies would displace sales of legitimate

72. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994).

73. 464 U.S. 417 (1984).

74. *See id.* at 420-21.

75. *Id.* at 456.

76. *Id.* at 442.

77. *Id.* at 444 (quoting Universal Studios, Inc. v. Sony Corp. of Am., 480 F. Supp. 429, 468 (C.D. Cal. 1979)).

recordings.[78] Congress responded, and in October 1992, President George Bush signed into law the Audio Home Recording Act (AHRA) of 1992.[79] The purpose of the legislation was to protect consumers from copyright infringement liability for taping (either video or audio) "copyrighted material for their own noncommercial, private use," while protecting copyright owners against widespread piracy.[80] To address proliferation of private copying, the AHRA both "adapt[ed] copyright law, and impose[d] a technical fix."[81] Specifically, the AHRA enumerated three components relating to the protection of both consumers and copyright owners.[82] First, copyright owners exchanged "all but the most slender thread of their claim" against private audio recording for royalties levied against producers of blank DATs and equipment.[83] Second, those who exercise "private" taping receive "immunity from copyright infringement actions, provided that the copying is performed on a digital audio copying device as defined by the AHRA."[84] And finally, manufacturers of all digital audio recording devices are required to implement a "Serial Copyright Management System" (SCMS) that will disable the device's ability to generate copies of any work it records, thereby controlling piracy via technology.[85]

3. The Internet and Copyright Legislation

Two recently enacted pieces of copyright legislation directly

78. *See* GORMAN & GINSBURG, *supra* note 52, at 511.

79. 17 U.S.C. §§ 1001-1010 (1994).

80. 137 CONG. REC. S21305 (daily ed. Aug. 1, 1991) (statement of Sen. DeConcini).

81. GORMAN & GINSBURG, *supra* note 52, at 511.

82. *See* ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT FOR THE NINETIES 459-60 (4th ed. 1993).

83. *See* GOLDSTEIN, *supra* note 1, at 163.

84. Robert A. Starrett, *Copying Music to CD: The Right, the Wrong, and the Law* (Feb. 1998) <http://www.emediapro.net/EM1998/starrett2.html>.

85. 17 U.S.C. § 1002 (1994); *see also* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d 624, 631-32 (C.D. Cal. 1998), *aff'd*, 180 F.3d 1072 (9th Cir. 1999). More specifically, § 1002 of the AHRA

> prohibits the manufacture, importation, or distribution of recording devices unless they are equipped with a Serial Copy Management System [SCMS], a system which permits the user of a digital recorder to make only one copy of digital source material. The objective is to permit unlimited copying from the original recording but to prevent second or third generation perfect copies of source material from being freely copied and distributed. In pursuit of that objective the Act prohibits the manufacture, importation, or distribution of any device that could circumvent the serial copy management system.

Kurlantzick & Pennino, *supra* note 65, at n.46.

address copyright infringement and digital music on the Internet.[86] The first is the Digital Performance Right in Sound Recording Act (DPRSRA) of 1995, which introduced a limited public performance right in sound recordings for Digital transmission on the Internet.[87] The second is the Digital Millenium Copyright Act (DMCA),[88] signed into law by President Clinton in October 1998,[89] which increased protection for copyrighted material on-line. While both acts pertain to digital music on the Internet, the DMCA addresses some of the issues that correspond to the ease of instant reproduction of multiple copies on the Internet, while the DPRSRA pertains only to performance rights.

There are two main issues addressed in the DMCA: Online Service Provider ("OSP") liability and anti-circumvention provisions. With respect to the first, Title II of the DMCA limits the liability of providers of on-line materials when copyright infringement is caused by third parties.[90] In addition, recently added section 512 grants OSPs limited protection from direct, contributory, or vicarious copyright infringement liability under certain circumstances.[91] The DMCA codified prior case law that held that OSPs could not be found "directly liable for copyright infringement when the OSP's system is merely a conduit for the spread of copyright-infringing materials."[92] OSPs could, however, be liable for third party activity through

86. A third piece of legislation, the No Electronic Theft Act ("NET") was enacted in 1997 to address computer-based piracy. *See* Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amendments to 17 U.S.C § 506 & 18 U.S.C. 2319). NET established criminal penalties for copyright infringement, regardless of profit motive. In November 1999, an Oregon college student pleaded guilty and was sentenced under NET to two years probation for posting pirated material (including 1,000 MP3 files) on his web site. *See* Jennifer Sullivan, *MP3 Pirate Gets Probation* (Nov. 24, 1999) <http://www.wired.com/news/mp3/0,1294,32276,00.html>.

87. Prior to the DPRSRA, the right of public performance was limited to songs (the underlying musical composition). Record companies were not entitled to collect fees from live performances or radio broadcasts because sound recordings do not have a general public performance right. *See* Bob Kohn, *A Primer on the Law of Webcasting and Digital Music Delivery*, 20 NO. 4 ENT. L. REP. 4, 10 (Sept. 1998); *see also generally* <http://www.kohnmusic.com>.

88. Pub. L. No. 105-304, 112 Stat. 2860 (1998).

89. *See* GORMAN & GINSBURG, *supra* note 52, at 550.

90. 17 U.S.C.A. § 512 (West Supp. 1999); *see also generally* Brandon Murai, Comment, *Online Service Providers and the Digital Millennium Copyright Act: Are Copyright Owners Adequately Protected?*, 40 SANTA CLARA L. REV. 285 (1999).

91. *See* Murai, *supra* note 90, at 288.

92. *Id.* at 287 (citing Playboy Enters., Inc. v. Webbworld, Inc., 991 F. Supp. 543 (N.D. Tex. 1997); Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997); Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167 (N.D. Ill. 1997); Religious Tech. Ctr. v. Netcom, 907 F. Supp. 1361 (N.D. Cal. 1995)).

contributory or vicarious copyright infringement.[93] The DMCA provides OSPs with a defense to possible infringement claims based on illegal acts committed by third party users. For example, one of the complex requirements in the DMCA allows copyright owners to demand that OSPs "take down" allegedly infringing material.[94] In return, OSPs will not be liable if they follow the "take down" procedures set forth in the Act.[95]

The second issue addressed in the DMCA resembles the AHRA in its complicated technological approach to preventing copyright infringement, by making it illegal to circumvent technological protection measures (such as SCMS) used by copyright owners to control access to their works.[96] There are three main provisions contained in the DMCA's anti-circumvention rules, addressing: (1) the *act of circumvention*, itself; (2) devices that circumvent *access controls*; and (3) devices that circumvent *copy controls*. The first of these rules is discussed in section 1201(a)(1)(A), which focuses on the *act of circumvention* and contains a general prohibition on circumvention of "a technological measure that effectively controls access to a work protected under this title."[97] The remaining rules focus on technologies capable of facilitating circumvention.[98] In particular, section 1201(a)(2) addresses devices and technologies that circumvent *access controls*, including technological measures "that effectively control[] access to a work protected under this title."[99] Similarly, section 1201(b)(1) addresses devices that circumvent *copy controls*, or, "protection afforded by a technological measure that effectively protects a right of a copyright owner... in a work or

93. *See* Murai, *supra* note 90, at 288 (citing Webbworld, Inc., 991 F. Supp. at 553-54; Hardenburgh, Inc., 982 F. Supp. at 514).

94. 17 U.S.C.A. § 512 (West Supp. 1999).

95. *Id.* § 512(b).

96. *See id.* §§ 1201-1205.

> (A) to "Circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner, and (B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

Id. §1201(a)(3)(A), (B).

97. *Id.* § 1201(a)(1)(A); *see also* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised,* 14 BERKELEY TECH. L.J. 525, 534 (1999).

98. *See* 17 U.S.C.A. §§ 1201(a)(2), (b)(1) (West Supp. 1999).

99. *Id.* § 1201(a)(2)(A).

portion thereof."[100]

This prohibition on circumvention of security measures is quite broad. In fact, the anti-circumvention provisions allow copyright owners to prevent access to their works that, under the Copyright Act, would not be infringing due to fair use.[101] For example, although the *Sony* Court deemed recording a television program for personal use on a VCR fair use, storing an audio or video file from the Internet on a hard drive for later listening and viewing may be prohibited under the DMCA if the owner of the copyrighted content places a "technological measure" that controls access to or restricts copying of the program. Moreover, the rights to works protected by technological measures under section 1201 are not necessarily subject to the same limitations on exclusive rights as under the Copyright Act. In other words, the DMCA anti-circumvention provisions potentially make illegal otherwise legitimate uses.

III. THE THREAT AND PROMISE OF DIGITAL AUDIO ON THE INTERNET

In order to understand the potential threat and promise of digital audio on the Internet, it is first necessary to consider the perspective of the current copyright stakeholders such as record companies represented by the RIAA. The music industry relies upon current copyright practice[102] because its income derives from record sales and copyright rules—rules which the recording industry lobbied strongly for—granting copyright owners exclusive rights in the reproduction and distribution of those pre-recorded media.[103] MP3 is not the first technology to threaten the music industry with piracy;[104] however, the

100. *See id.* § 1201(b)(1)(A).

101. *See* 144 CONG. REC. E2136-37 (daily ed. Oct. 13, 1998) (statement of Rep. Tom Bliley, Chairman of the Committee on Commerce, warning that "under section 1201(b)... a copyright owner could successfully block the manufacturing and sale of a device used to make fair use copies of copyrighted works, effectively overruling the Supreme Court's landmark decision in *Sony Corp. of Am. v. Universal Studios, Inc.*, 464 U.S. 417 (1984).").

102. *See* NIMMER, *supra* note 65.

103. "During the 105th Congress that ended in October 1998, the RIAA was a leading voice on issues that included... [the] World Intellectual Property Organization Treaties & The Digital Millennium Copyright Act." *Legislation RIAA Online* (visited Mar. 18, 2000) <http://www.riaa.com/musicleg/ml_fed.htm>.

104. Devices embodying MPE technology pose some issues which are strikingly similar to the player piano in the early 1900's, as well as to other earlier generations of new media. *See* White-Smith Music Publishing Co. v. Apollo Co., 209 U.S. 1 (1908) (player pianos); *see* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984) (videocassette recorders); *see also* David Segal, *Blame it on Rio (Music Industry Litigators Do)*, WASH. POST, Nov. 16, 1998, at F9 (stating that "CDs are essentially software and therefore are as easy to pirate as floppy disks.").

digital format, in general poses some unique threats.

According to some, the recording industry believes that mass reproduction and distribution of digital audio files pose a much larger threat than reproduction of a CD onto cassette tapes because digital audio files can be perfectly copied, with little or no loss of quality.[105] Consequently, unlike people who use traditional duplication methods, recipients of digital copies of musical works may lack the impetus to purchase an authorized CD. The Internet, MP3 compression technology, and technologies that help locate and transfer music digitally further enhance the attractiveness of downloading digital audio files.

Thus far, the Internet has developed largely without regulation, lacking any valid authority capable of policing on-line communications and commerce.[106] In fact, one commentator has even observed that the Internet is an "inherently anarchistic place where copyright doesn't apply."[107] Therefore, many Internet users tend to believe that everything available over the Internet, including music, is free.[108] As a result of this misconception, the music industry has found itself "up against an international medium that is not ruled by any one country's laws," a medium that developed as a share-and-share-alike environment.[109] Because the recording industry relies upon record sales for revenue, it fears that music fans on the Internet, accustomed to utilizing the vast resources, products, and services at no cost, will choose to obtain unauthorized music for free, rather than paying for legitimate copies.[110]

---

105. *See generally* I. TROTTER HARDY, UNITED STATES COPYRIGHT OFFICE, PROJECT LOOKING FORWARD: SKETCHING THE FUTURE OF COPYRIGHT IN A NETWORKED WORLD (May 1998) <http://lcweb.loc.gov/copyright/cpypub/thardy.pdf>.

106. *See* CONNER-SAX & KROL, *supra* note 4, at 8 ("[T]he Internet's commercial growth is largely governed by the invisible hand of the free market. . . . the U.S. government never really played a significant role in governing the Internet."). While the government initially maintained a fairly hands-off approach to ensure that a relatively unencumbered growth of the Internet (*see generally* Reno v. ACLU, 521 U.S. 844 (1997)), regulations pertaining to the Internet and e-commerce have evolved more haphazardly in the past two years. For a summary of current and pending legislation relating to the Internet, *see All About the Internet: Legislation* (visited Mar. 8, 2000) <http://www.isoc.org/internet/law/legis.shtml>.

107. Pauline Tam, *An On-Line Link to Top Tunes is Soon to Boom: On-Line: Music Industry Faces Anarchy of the Internet Independents*, VANCOUVER SUN, Aug. 2, 1994, at C4 (quoting Rob Lord of the Independent Underground Music Archive saying, "The Net is too beautiful a place. It's a cooperative, anarchistic system. The values that the music industry tries to superimpose onto the Internet don't apply.").

108. *See* Charap & Rothstein, *supra* note 13.

109. Lipton Krigel, *supra* note 9.

110. *See Testimony of Hilary Rosen, supra* note 26 (stating, "Of course, one thing that distinguishes music from most other products is that you can not only market and sell it

Contrary to the recording industry's concerns, however, not all uses of MP3 technology infringe. Reproduction and distribution (both legitimate and infringing), can occur at virtually no marginal cost.[111] For example, because the Internet serves as a legitimate way to generate revenue and reach consumers with marketing information and direct sales,[112] the same factors that threaten the recording industry and facilitate piracy—fidelity, compressibility, and malleability—also provide unconstrained market entry for independent record companies and individual musicians.[113] Similarly, the Internet allows artists to reach their audience directly.[114] What might be a threat to the status quo in the recording industry could present promising opportunities for independent labels and musicians.[115]

A. The Cases

In response to the perceived threat of the MP3 format, the recording industry has initiated several legal actions alleging digital music piracy.[116] Three cases in particular were filed by the RIAA.[117]

---

online . . . you can actually deliver it, instantly, through the very same channel.").

111. *See* Eric Schlachter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could be Unimportant on the Internet, Symposium*, 12 BERKELEY TECH. L.J. 15, 20 (1997) (noting that "the costs of making one extra copy of intellectual property on-line are insignificant.").

112. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1074 (9th Cir. 1999) (noting that "the Internet also supports a burgeoning traffic in legitimate compressed audio files. Independent and wholly Internet record labels routinely sell and provide free samples of their artist's work online, while many unsigned artists distribute their own material from their own websites."); *see also* Robert MacMillan, *MP3.com Blasts RIAA at High Volume*, NEWSBYTES, Oct. 12, 1998, *available in* 1998 WL 20717326 (quoting Michael Robertson of music download site MP3.com: "[t]he (online music) market is already well underway, and that [sic] just because (the RIAA) is not controlling it does not mean that it does not exist and is not flourishing—legitimately.").

113. "MP3 threatens the music industry in other ways that are ultimately more interesting that bootleg reproductions of copyrights material." CONNER-SAX & KROL, *supra* note 4, at 364.

114. Direct access to audiences is another threat to the established business model the recording industry has built because it has the potential to remove the bottleneck, the necessity of the record companies themselves. *See Making an Ally of Piracy*, N.Y. TIMES, May 9, 1999, §2 at 50 ("It used to be that a label was needed to finance, manufacture, store, ship and market your music. . . . but in the digital era, it costs nothing to ship your music over the Internet to a fan." (quoting Jaron Lanier's manifesto "Piracy is Your Friend.")); *see also* CONNER-SAX & KROL, *supra* note 4, at 362.

115. *See* MacMillan, *supra* note 112 (in discussing RIAA's response to alternatives that now compete with the record labels, MP3.com's President Michael Robertson states, "The train has already left the station. Now they want to derail it. None of the 'A's' in RIAA stand for artists. They support the record industry.").

116. *See* Brown, *supra* note 39 ("An RIAA lawsuit has become almost a coming-of-age ritual for online music companies attempting some new form of digital music distribution.").

In the first case, *The Recording Industry Ass'n of America v. Diamond Multimedia Systems, Inc.*[118] (the *Rio* case), plaintiff RIAA sued Diamond Multimedia under the AHRA.[119] After the *Rio* case

117. At least one other case has been filed that involves digital music distribution on the Internet. A federal case filed in Washington, RealNetworks v. Streambox involves the anti-circumvention provisions of the DMCA and various other intellectual property claims. *See* Sara Robinson, *3 Copyright Lawsuits Test Limits of New Digital Media* (Jan. 24, 2000) <http://search.nytimes.com/search/daily/homepage/bin/fastweb?getdoc+cyber-lib+cyberlib+9767+1+wAAA+mp3>. *See Compl. for Violation of the Digital Millenium* [sic] *Copyright Act, Contributory, Vicarious and Direct Copyright Infringement, Tortious Interference with Contract, Consumer Protection Act Violation and Lanham Act Violations,* RealNetworks, Inc. v. Streambox, Inc. (Wash. 1999) (No. C99-2070Z), *available at* (visited Mar. 15, 2000) <http://www.realnetworks.com/company/pressroom/pr/99/rnwk_complaint.html>; *see also Response of Def. Streambox, Inc. to Pl.'s Mot. for Temporary Restraining Order and Order to Show Cause,* RealNetworks, Inc. v. Streambox, Inc. (Wash. 1999) (No. C99-2070P) *available at* (visited Mar. 15, 2000) <http://www.streambox.com/RNvsSB/StreamboxResponse.htm>; *see also Order On Pl.'s Mot. for Prelim. Inj.,* Realnetworks, Inc. v. Streambox, Inc. (Wash. 1999) (No. C99-2070P), *available at* (visited Mar. 15, 2000) <http://www.realnetworks.com/company/pressroom/pr/streambox/courtorder_011800.html>.

Additionally, while not directly addressing MP3, three cases have been filed on behalf of the motion picture industry regarding a DVD playback utility for the Linux operating system called DeCSS with the potential to impact digital media and intellectual property law on the Internet. The Motion Picture Association of America (MPAA) sued three individuals alleging violation of the DMCA by "proliferating a software device that unlawfully defeats the DVD copy protection and access control system." *Compl. for Violation of Provisions Governing Circumvention of Copyright Protection Systems, 17 U.S.C. Section 1201, et. seq.,* Universal City Studios, Inc., et. al. v. Shawn C. Reimerdes, et. al. (S.D.N.Y. 2000) (No. 00cv00277), *available at* (visited Mar. 15, 2000) <http://www.eff.org/ip/Video/MPAA_DVD_cases/20000114_mpaa_ny_complaint.html>; In particular, eight major motion picture studios filed suit in New York stemming from the discovery and proliferation of a computer program that "unlawfully defeats the DVD copy protection . . . so that individuals can make, distribute, and/or otherwise electronically transmit or perform unauthorized copies of Plaintiff's copyrighted motion pictures and other audiovisual works." *Id. See also Prelim. Inj.,* Universal City Studios, Inc., et. al. v. Shawn C. Reimerdes, et. al., *available at* (visited Mar. 15, 2000) (S.D.N.Y. 2000) (No. 00 Civ. 0277), <http://www.eff.org/ip/Video/MPAA_DVD_cases/20000120_pi_order.html>.

A related case was brought on behalf of the organization that licenses the encryption technology and claimed only a California trade secret violation. *See Compl. for Injunctive Relief for Misappropriation of Trade Secrets,* DVD Copy Control Ass'n v. Andrew Thomas McLaughlin, et. al. (Cal. Super. Ct. 2000) (No. CV786804), *available at* (visited Mar. 15, 2000) <http://www.eff.org/ip/Video/DVDCCA_case/19991228-complaint.html>; *see also Def.'s Mem. of P. & A. in Opp'n to Order to Show Cause Re: Prelim. Inj.,* DVD Copy Control Ass'n v. Andrew Thomas McLaughlin, et. al. (Cal. Super. Ct. 2000) (No. CV786804), *available at* (visited Mar. 15, 2000) <http://www.eff.org/ip/Video/DVDCCA_case/20000107-pi-motion-response.html>; *Order Granting Prelim. Inj.,* DVD Copy Control Ass'n v. Andrew Thomas McLaughlin, et. al. (Cal. Super. Ct. 2000) (No. CV786804), *available at* (visited Mar. 15, 2000) <http://www.eff.org/ip/Video/DVDCCA_case/20000120-pi-order.html>.

118. 180 F.3d 1072 (9th Cir. 1999).

119. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d 624 (C.D. Cal. 1998), *aff'd,* 180 F.3d 1072 (9th Cir. 1999).

settled, a flurry of cases were also filed that may help sort out some of the ambiguities pertaining to Internet music and copyright law. In particular, the RIAA sued Napster in December 1999, alleging contributory and vicarious copyright infringement.[120] Then, in January 2000, the RIAA filed suit against MP3.com claiming violation of the exclusive right to make reproductions of its sound recordings.[121] Although the issues in these cases are complex and unresolved, they illustrate the conflicts between the recording industry and consumers as well as highlight critical policy issues involved with intellectual property rights and music on the Internet.[122]

1. RIAA v. Diamond

On October 9, 1998, the RIAA filed a complaint in the United States District of the Central District of California against Diamond Multimedia, claiming Diamond's portable Rio MP3 player[123] violated the AHRA. The RIAA argued that the Rio would "harm [the RIAA] and the public interest by dramatically stimulating the traffic in illegal MP3 files."[124] More specifically, the RIAA asserted in its complaint that "because the overwhelming majority of MP3 music files on the Internet are unauthorized," the Rio would "facilitate and encourage the unlawful trafficking of infringing MP3 music files."[125] The RIAA also pleaded that the proliferation of pirated sound recordings threatened the music industry by discouraging consumers from purchasing legitimate recordings.[126] However, the RIAA limited its claim to the lone assertion that the *Rio* did not comply with the

120. *See* Mike France, *This Lawsuit is Cranking Up the Volume Over MP3* (Dec. 13, 1999) <http://www.businessweek.com/cgi-bin/ebiz/ebiz_frame.pl?url=/ebiz/9912/ep1213.htm>.

121. *See* Robinson, *supra* note 117.

122. *See id.* (noting that the recent cases reveal a "growing conflict between the entertainment industry, which is struggling to protect its products and profits in the Internet age, and consumer groups, which accuse the industry of interfering with free speech and people's rights to control their watching or listening experience.").

123. *See* discussion *supra* Part II.B. for a description of the Rio.

124. Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d 624, 632-33 (C.D. Cal. 1998), *aff'd*, 180 F.3d 1072 (9th Cir. 1999). Until the *Rio* rendered MP3 files portable, MP3 users were limited to listening to their music files at their computers. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1074 (9th Cir. 1999).

125. *Compl. for Violation of the Audio Home Recording Act*, Recording Indus. Assoc. of Am. & Alliance of Artists and Recording Cos. v. Diamond Multimedia Sys., Inc. (C.D. Cal. 1998) (No. 98-8247), *available at* <http://www.riaa.com/piracy/pir_pr.htm>.

126. Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d at 1074. The RIAA predicts that "losses to digital Internet piracy will soon surpass the $300 million that is allegedly lost annually to other more traditional forms of piracy." *Id.*; *see also id.* at n.1.

requirements set forth in the AHRA,[127] and did not allege a copyright infringement claim against Diamond.[128]

The RIAA, in an attempt to deter other manufacturers of MP3 devices and to buy some time to sort the issues while preparing for trial, included in its complaint *ex parte* application enjoining Diamond from manufacturing and shipping the *Rio* MP3 player.[129] After oral arguments, the court issued a temporary restraining order enjoining Diamond from manufacturing or distributing the *Rio* player.[130] However, on October 26, 1998, the District Court denied the RIAA's motion for preliminary injunction, holding that "because the *Rio* is capable of recording legitimate digital music, an injunction would deprive the public of a device with significant beneficial uses."[131]

Following the District Court's ruling, the portable MP3 player entered the market for the 1998 holiday season.[132] Six months later, in June 1999, The Court of Appeals for the Ninth Circuit issued its opinion on the RIAA's appeal of the District Court's denial of preliminary injunction.[133] The Court found that the *Rio* "is not a digital audio recording device subject to the restrictions of the [AHRA]" and upheld the District Court's denial of the preliminary injunction.[134] Following the Ninth Circuit's ruling and without

127. *See* 17 U.S.C. §§ 1002-1004 (1994) (setting forth the copying control and royalty payment requirements of devices that fall under the AHRA).

128. Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d at 627 (citing *Sony* and noting that "even if the *Rio* is not subject to the AHRA and therefore subject to the Copyright Act—Defendant has a potential 'fair use' defense that might defeat any prima facie showing of infringement."); *see also* Charap & Rothstein, *supra* note 13 (speculating that "the RIAA omitted a copyright claim because it was wary of another Betamax decision—i.e. because the *Rio* device can transport pirated and legal audio files, it arguably has substantial non-infringing uses.").

129. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d at 626.

130. *See id.*

131. *Id.* at 633.

132. *See Diamond Press Release*, *supra* note 34. Since December 1998, sales of the *Rio* and other portable MP3 players has intensified. *See* Freund, *supra* note 7, at 136 (noting that "[i]n the meantime, copyright squabbles aren't slowing the slew of competitors" and reporting on various MP3 players from a variety of manufacturers.). *But see Morning Edition, MP3 Devices to Record Music Via the Internet Not as Popular as Predicted and Music Companies are Still Arguing Over the Right to Copy Music From Their Artists* (National Public Radio broadcast, Nov. 15, 1999) *available in* LEXIS, National Public Radio Library. [hereinafter *Morning Edition*] (reporting that "[e]arlier this year, analysts were saying that by the holidays there'd be a dozen different MP3 players available. Instead, there are three.").

133. *See generally* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072 (9th Cir. 1999).

134. *Id.* at 1081 (noting that "a device falls within the [AHRA's] provisions if it can

releasing any terms, Diamond and the RIAA settled their case.[135]

Although the Ninth Circuit's decision settled the question of whether the *Rio* was subject to the AHRA and led to the end of the RIAA's fight against the *Rio*, the following cases demonstrate that the RIAA's fight against the MP3 format and piracy on the Internet has not ceased.[136]

2. RIAA v. Napster

On December 7, 1999, the RIAA brought a federal copyright action against Napster in California alleging contributory and vicarious copyright infringement for enabling Napster users to trade pirated music.[137] The RIAA is seeking up to $100,000 per copyrighted song exchanged by way of the Napster program, claiming that "Napster is about facilitating piracy, and trying to build a business on the backs of artists and copyright owners."[138] The Napster program places the RIAA in a difficult situation because the music exchanged via Napster is not stored on central servers, but on the computers of individual users. This aspect presents too many users for the RIAA to effectively pursue individually.[139]

At this time, neither the RIAA complaint nor Napster's response to the RIAA's charges are generally available. However, this case

---

indirectly copy a digital music recording by making a copy from a transmission of that recording. Because the *Rio* cannot make copies from transmissions, but instead, can only make copies from a computer hard drive, it is not a digital audio recording device.").

135. *See* Chris Oakes, *RIAA, Diamond Sweep Away Suit* (Aug. 4, 1999) <http://www.wired.com/news/print/0,1294,21089,00.html>; *see also* Charap & Rothstein, *supra* note 13, at n.10 (quoting Diamond's general counsel, Ron Moore, saying, "Diamond Multimedia and our RioPort subsidiary are pleased to bring an end to this legal dispute as we move forward with the music industry on the development of secure e-commerce music offerings through [SDMI].").

136. The RIAA fights a constant battle, monitoring and shutting down Internet sites with illegal MP3 files. *See RIAA Releases 1999 Midyear Anti-Piracy Statistics* (Aug. 17, 1999) <http://www.riaa.com/piracy/pir_pr.htm##_top> ("In the first six months of 1999, the RIAA's Internet enforcement team sent thousands of cease and desist and educational letters to sites offering unauthorized songs for download."); *see also Get Your Hands Off Our Music*, (Dec. 8, 1999) <http://www.wired.com/news/print/0,1294,32977,00.html> (reporting on the recent suit filed against Napster. The article states that the RIAA, "angered by the ease with which visitors to Napster.com can download and share music files, has filed a copyright infringement suit against the music software company.").

137. *See* France, *supra* note 120.

138. Jack McCarthy, *Studios Sue MP3 Startup Napster* (Dec. 9, 1999) <http://www.cnn.co.jp/1999/TECH/computing/12/09/napster.suit.idg/index.html> (quoting Cary Sherman, general counsel of the RIAA).

139. *See* Scott Rosenberg, *The Napster Files* (Feb. 4, 2000) <http://www.salon.com/tech/col/rose/2000/02/04/napster_swap/index.html>.

has been widely covered in the media and is bound to address some of the controversy of on-line music. There is no doubt that people can and do use Napster to trade copyrighted music. Is Napster responsible for the illegal activities of its individual users? If Napster can establish that third-party material merely passes through its system, it may escape liability entirely.[140] Otherwise, as an OSP, Napster will probably claim that it has limited liability under the DMCA for the infringing activities of its members.[141] In order to hold Napster responsible for the acts of its members, the RIAA will have to prove that Napster had "actual knowledge" that material it refers or links users to contained copyright material and was infringing.[142]

Another argument available to Napster is the invocation of the *Sony* case to support a defense that Napster cannot be liable for contributory infringement because it is a program that facilitates substantial non-infringing uses.[143] Although a more thorough exploration of the issues of this case is beyond the scope of this comment, the dispute is worth watching because of the critical policy issues it raises. While copyright owners are justified in trying to protect their intellectual property from piracy on the Internet, holding Napster responsible for the infringing actions of its users could upset the balance sought by copyright law, thereby posing a substantial burden upon a variety of companies that provide directory and search services to copyrighted materials available on-line.[144]

3. RIAA v. MP3.com

The RIAA filed suit in New York against MP3.com on January 21, 2000 alleging that MP3.com's new "My.MP3.com" service violates copyrights owned by record companies that the RIAA represents.[145] MP3.com claims that its "Beam-It" software program, which recognizes CDs in a customer's CD-ROM drive, acts "sort of

140. Specifically, to qualify as "Transitory Digital Network Communications," Napster must not (1) initiate the transmission; (2) select the material; (3) select recipients for the transmission; (4) make or keep copies for longer than the time it takes to transmit or route; or (5) alter the content. 17 U.S.C.A. § 512(a) 1-5 (West Supp. 1999).

141. *See* discussion *supra* Part II.C.3. for a brief description of OSP immunity under the DMCA.

142. *See* 17 U.S.C.A. § 512(d) (West Supp. 1999) for a description of the DMCA provisions regarding OSP liability and "Information Location Tools."

143. *See* Brown, *supra* note 39.

144. *See generally id.*

145. *See Compl. For Copyright Infringement,* UMG, Inc., et. al. v. MP3.com, Inc. (S.D.N.Y. 2000) (No. 00 Civ. 0472), *available at* (visited Mar. 16, 2000) <http://www.mp3.com/news/533.html?hparticle2>; *see also* Robinson, *supra* note 117.

like a license" to access the music in the MP3.com database.[146] Conversely, the RIAA alleges that MP3.com has no license to the music that it catalogues for playback to its customers. In an open letter to MP3.com's CEO Michael Robertson, RIAA president Hillary Rosen stated, "[i]t is not legal to compile a vast database of our member's sound recordings with no permission and no license. And whatever the individual's right to use their own music, you cannot exploit that for your company's commercial gain."[147]

In response to the RIAA's allegations, MP3.com claims that it has implemented sufficient security features to prevent unauthorized copying and that the service is merely another version of the time-shifting practices authorized by the Court in *Sony*.[148] MP3.com's Robertson asserts that consumers have the right to listen to digital music files if they have already paid for the CD and poses the question: "You don't have to pay more royalties to listen to a CD in your living room; why should you pay more royalties to listen to your CD in your living room on your computer?"[149] Whether MP3.com will ultimately prevail under a fair use defense—that the My.MP3.com service is equivalent to making a copy for personal use—remains to be determined.

B. Outlook

According to copyright expert Paul Goldstein, copyright owners usually suffer and consumer electronics companies usually benefit while Congress and the courts delay rulemaking regarding home copying.[150] In fact, one major reason for the court's denial of the injunction in the *RIAA v. Diamond* case is that the risk of harm to the record companies posed by the *Rio* was greatly outweighed by the interest of promoting emerging technology.[151] Although the *Rio* case

146. Brown, *supra* note 39 ("The RIAA's lawsuit here hinges around the invisible machinations behind Beam-It: Whenever you 'beam' a CD into your account, someone at MP3.com is actually running out and buying that CD and ripping it for you. MP3.com has amassed and ripped a collection of 45,000 CDs to have at the ready.").

147. Letter from Hilary Rosen, President and CEO, RIAA, to Michael Robertson, CEO, MP3.com (Jan. 21, 2000) <http://www.mp3.com/response2.html>.

148. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 418 (1984).

149. Brown, *supra* note 39.

150. *See* GOLDSTEIN, *supra* note 1, at 134.

151. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d 624, 633 (C.D. Cal. 1998), *aff'd*, 180 F.3d 1072 (9th Cir. 1999) (emphasizing that the evidence offered by Diamond showed "an injunction would substantially impact... at a minimum... multi-million dollar losses" of revenues collected in the sale of the *Rio*; denying the injunction because the court felt the *Rio* was a device with "significant beneficial uses.").

settled, the pending litigation is convincing evidence that the RIAA remains afraid that as time passes and more consumers embrace the flexibility of the MP3 format, the expectation of free copying will proliferate.[152]

1. The Law

Congress has faced the difficult task of predicting effects of new technology on the marketplace. Robert Kastenmeier, chair of the House Intellectual Property subcommittee prior to the Copyright Act of 1976 Act, articulated this difficulty, stating, "if you wait until the problem is mature, the industrial interests that are posed one against another may be so significant [that it is much more difficult to transcend them without] destroying one party commercially or financially, than it would be had you anticipated the problem years before."[153] With the passage of the 1976 Act, Congress intended to ensure that copyright laws could potentially apply to emergent, possibly unimagined, new technologies:[154]

> Authors are continually finding new ways of expressing themselves, but it is impossible to foresee the forms that these new expressive methods will take. The [1976 Act] does not intend either to freeze the scope of copyrightable subject matter at the present stage of communications technology [or to establish a limitless framework].[155]

In considering whether to adjust the Copyright Act in the face of emerging technology, including the Internet, a recent report entitled Intellectual Property Rights on the National Information Infrastructure ("White Paper")[156] by the Clinton Administration's Information Infrastructure Task Force (the "Task Force") recognized that:

> When technological advances cause ambiguity in the law, courts look to the law's underlying purposes to resolve that ambiguity. However, when technology gets too far ahead of the law, and it

152. GOLDSTEIN, *supra* note 1, at 134.

153. *Id.*

154. *See* JON A. BAUMGARTEN ET AL., BUSINESS & LEGAL GUIDE TO ONLINE-INTERNET LAW 205 (1997).

155. *Id.* (quoting H.R. REP. NO. 94-1476 at 51 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5664).

156. INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT ON THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS (Sept. 1995) (Bruce Lehman & Ronald H. Brown, Chairs) [hereinafter WHITE PAPER].

> becomes difficult and awkward to adapt the specific statutory provisions to comport with the law's principles, it is time for reevaluation and change.[157]

The White Paper concluded that existing copyright law is flexible enough to adapt to inevitable changes in circumstances, and predicted that only limited adjustments would be necessary.[158]

It is arguable whether or not the update to the Copyright Act included in last year's DMCA constitutes the "limited adjustments" contemplated by the Task Force. For instance, with the anti-circumvention provisions in the DMCA, Congress introduced a "novel concept into copyright law—for the first time, the law protects not only the copyrighted work, but the means that are used to control access to that work."[159] Copyright is said to be a "bargain" between the public and copyright holders.[160] Prior to the DMCA anti-circumvention provisions, neither Congress nor the courts had relinquished control to copyright owners over "looking at, listening to, learning from, or using copyrighted works."[161] This has lead copyright experts to ask if this type of copyright protection, that potentially burdens the public, is necessary as an incentive to creative production?

The success of the Internet has been attributed to "both satisfying basic community needs as well as utilizing the community in an effective way to push the infrastructure forward."[162] The notion of private individuals all over the world swapping digital music, having access to an entire music collection from anywhere on the Internet, and copying those MP3 files onto portable media, is no longer a mere vision of the future. Although the anti-circumvention provisions in the DMCA may seem like a reasonable response to the threat of piracy in the digital age, the new laws might actually retard growth of

---

157. *Id.* at 211.

158. *Id.* at 90-95.

159. *WIPO The DMCA One Year Later: Assessing Consumer Access to Digital Entertainment on the Internet and Other Media: Hearing Before the Subcomm. on Telecommunications, Trade, and Consumer Protection, Comm. on Commerce,* 106th Cong. 29 (1999) (statement of Peter Harter, Vice President, Global Public Policy and Standards, EMusic.com), *available in* LEXIS, Federal Document Clearing House Congressional Testimony File [hereinafter *Harter Testimony*].

160. Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract And Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827, 855 (1998); *see generally* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29 (1994).

161. Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19, 35 (1996) [hereinafter Litman, *Revising Copyright Law for the Information Age*].

162. ISOC, *supra* note 16.

digital media and the Internet.[163] Along these lines, Berkeley law professor Pamela Samuelson warns that:

> [C]ultivating good citizenship is probably a better idea than trying to mandate that every piece of technology can't play something for which there is no authorization. In some sense you have to think through your long-term strategy. The kind of Draconian measures it would take to stop [piracy] would make us a copyright police state which we wouldn't want to live in.[164]

With the recent emergence of affordable high performance computers and high-speed Internet connections, the RIAA seems to have positioned itself against digital audio technology rather than embracing its continuing development.[165] The recording industry would most likely prefer that any new copyright rules support continued dominance in the marketplace.[166]

2. "Securing" Digital Music

In denying the RIAA's appeal of the District Court's ruling on the preliminary injunction, the Ninth Circuit concluded that the *Rio* is not a "Digital Audio Recording Device" as defined by the AHRA.[167] Therefore, the Rio MP3 player was not required to "comply with the SCMS requirement."[168] While not required, the recording industry's approach to fighting piracy (in addition to litigation) has been to develop copyright management systems, technological measures to limit piracy, that it hopes will be adopted industry-wide. Along these lines, in December 1998, the RIAA, consumer electronics companies (including *Rio* manufacturer, Diamond), and Internet Music representatives, formed the Secure Digital Music Initiative (SDMI), a

163. *See Harter Testimony*, *supra* note 159 (suggesting that the DMCA, a "law designed to foster the growth of digital media may, in fact, have just the opposite result.").

164. Leonard, *supra* note 12 (quoting U.C. Berkeley law professor Pamela Samuelson).

165. *See* Peraino, *supra* note 50, at 144-45 (discussing the RIAA's legal attempts to block the *Rio* in 1998 and DAT recorders in 1990).

166. In fact, the RIAA was a leading voice in the formation of the DMCA. *See* <http://www.riaa.com/musicleg/ml_fed.htm>; *see also* Litman, *Revising Copyright Law for the Information Age supra* note 161, at 25.

167. *See generally* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1078 (9th Cir. 1999). The court focused primarily on the fact that the *Rio* only "recorded" from a computer hard drive, that "the *Rio* merely makes copies in order to render portable, or 'space-shift,' those files that already reside on a user's hard drive.... Such copying is paradigmatic noncommercial personal use...." *Id.* at 1079. The court also noted the fact that the *Rio* "does not permit such further copies to be made because it simply cannot download or transmit the files that it stores to any other device." *Id.*

168. *Id.* at 1078.

forum to develop technological standards to limit consumers' ability to copy digital music in MP3 and other digital music formats.[169]

Since its formation in late 1998, SDMI has been meeting worldwide but failed to meet its goal of having SDMI-compliant products available for the 1999 holiday season and continues to finalize its standards.[170] SDMI has provided some guidelines for distribution of on-line music but the future of SDMI is uncertain.[171] One approach to securing digital music is to develop technologies that control how digital music is used after purchase, such as limiting the number times a consumer can copy, play or distribute digital copies.[172] As more secure formats become available, it is predicted that more music from the major record labels and more consumer electronic devices to playback MP3 formatted music files will become available.[173]

---

169. SDMI was announced at a press conference by Hilary Rosen, President and CEO of the RIAA, in December 1998. *See Worldwide Recording Industry Announces Precedent-Setting Initiative to Address New Digital Music Opportunities* (Dec. 15, 1998) <http://www.riaa.com/tech/tech_pr.htm>. SDMI consists of "more than 120 companies and organizations representing a broad spectrum of information technology and consumer electronics businesses, Internet service providers, security technology companies and members of the worldwide recording industry." *SDMI Fact Sheet* (visited Mar. 15, 2000) <http://www.sdmi.org/public_doc/FinalFactSheet.htm>. SDMI serves as a

> forum for these industries to develop the voluntary, open framework for playing, storing and distributing digital music necessary to enable a new market to emerge. SDMI is working on two tracks. The first has already produced a standard, or specification, for portable devices. The longer-term effort is working toward completion of an overall architecture for delivery of digital music in all forms. *Id.*

170. *See* Michael Learmonth, *CD, Cassette – Or Download?* THE STANDARD (Mar. 6, 2000) <http://www.thestandard.com/article/display/0,1151,12466,00.html>.

171. *See Morning Edition, supra* note 132 (reporting that Phase I only distinguishes "between music... that was released before SDMI and that which will come after. It does this by requiring an inaudible digital signal to be imbedded in any music that's released from now on. The major labels will start including it soon."); *see also* Stephanie Miles, *Infighting Threatens to Kill Net Music Antipiracy Standard,* (Sept. 23, 1999) <http://news.cnet.com/category/0-1005-200-122852.html> (quoting Sony Vice President Geoffrey Anderson's email message to SDMI members: "Despite the months of hard work by the SDMI participants, SDMI portable device manufacturers and SDMI service providers are still unable to prepare for this holiday season.... We will be deeply disappointed if continued delays within SDMI frustrate the goals of implementers and SDMI alike.").

172. *See* Christopher Jones, *RIAA-Friendly Rio Surfaces* (Mar. 16, 2000) <http://www.wired.com/news/print/0,1294,35003,00.html>.

173. *See id.* Some critics predicted that portable MP3 devices would be popular regardless of SDMI. *See* Eric Scheirer, *The End of SDMI* (Oct. 15, 1999) <http://www.mp3.com/news/394.html> (stating that "[t]he floodgates are opening. Portable devices will be huge for Christmas this year; they will all play MP3, and none of them will be SDMI-compliant in any way that matters."). Some commentators, however, suggest that MP3 players have been "slow to take off because they've raised fundamental questions about the way

Not all members of the on-line music community embrace the SDMI copyright management specifications.[174] Critics of SDMI assert that the music industry will use SDMI standards to leverage its distribution power and to maintain control.[175] The concern is that SDMI will be a proprietary standard that, along with the DMCA's anti-circumvention provisions, will reduce copyright holders' ability to "authorize distribution of their works" as they see fit, while allowing for consumers' right to fair use.[176]

Because services and technologies like the Rio, Napster, and My.MP3.com have made it possible to embody music in this new medium, songwriters, publishers, and record companies are recognizing common interests that have spurred them to reach formal and informal compromises with regard to on-line copyright problems.[177] SDMI, along with other copyright management systems in development are examples of non-judicial, non-legislative approaches addressing piracy concerns.[178] Whether the RIAA will

---

the music industry distributes its product." *Morning Edition, supra* note 132.

174. In fact, some claim the standard is "doomed." *See* Jane Wakefield, *Rival Predicts Death for SDMI Standard* (last modified July 11, 1999) <http://www.zdnet.com/zdnn/stories/news/0,4586,2290381,00.html>, *available in* 1999 WL 14793573 (quoting Bob Kohn, chairman of Emusic.com, saying that "MP3 is the operating system of digital downloads.... In a year's time, the SDMI standard will suffer the same demise as Divx. The standards war is over today.").

175. Beth Lipton Krigel, *Music Initiative Raises Questions* (Dec. 16, 1998) <http://news.cnet.com/news/0-1005-200-336464.html?tag=st.cn.1> (quoting online record company spokesman Steve Grady's reaction to the RIAA's announcement in December 1998: "The announcement was not at all about security or about piracy—it's about control.... By implementing security, they maintain control."); *see also* Scheirer, *supra* note 173 (stating that SDMI is not "just about providing security options to the musician, though. It [is] about providing security options that [are] controlled by the music industry.").

176. *See generally Electronic Frontier Foundation Digital Audio and Free Expression Policy Statement, supra* note 13. In May 1999, the Electronic Frontier Foundation (EFF), the Internet's "leading free-expression political action group," held its first meeting of the Consortium for Audiovisual Free Expression (CAFE), to bring together a group of musicians, technologists, entrepreneurs, and attorneys to "refine a platform, develop educational and legal strategies to protect open standards in the digital music space, and counter recording industry efforts to limit those standards." *See* James Glave, *Music for the Masses*, (May 26, 1999) <http://www.wired.com/news/politics/0,1283,19884,00.html>.

177. *See* Neuburger & Israel, *supra* note 2, at C17. One compromise provides that

> the holder of the copyright in a sound recording may allow 30-second downloads without incurring a mechanical licensing obligation to the holder of the copyright in the underlying composition, if the downloads promote the sale of the recording. Similarly, the holder of the copyright in the underlying composition may allow 30-second downloads without incurring an obligation to the holder of the copyright in the sound recording, again provided that the downloads promote the sale of the recording. *Id.*

178. *See* Glave, *supra* note 176.

come to a similar collaborative compromise in its suits against Napster and MP3.com remains to be seen. The Napster and MP3.com cases are rooted in the RIAA's concern about the future of digital music distribution. Both technologies offer users control over collecting, exchanging and listening to music, and they are both means of music distribution and transmission that do not necessarily originate with the recording industry.[179]

IV. CONCLUSION

Even with advanced technological measures, like SDMI, some "pirates will always be able to crack such protection."[180] Because the latest digital technologies facilitate unlimited reproductions with little or no loss of sound quality, copyright owners legitimately fear that their works will be freely copied and disseminated without compensation, in violation of copyright law.[181] Consequently, it is not surprising that each time a new digital music technology emerges, the recording industry attempts to limit its release.[182] Perhaps the problem with MP3 is that it is too late—"the horse is already out of the barn."[183] Too often, the ire is misdirected towards technology, rather than the people who use the technology. In other words, players do not pirate, pirates pirate.[184]

As copyright management standards are developed and the DMCA is both implemented and interpreted, the balance of private and public interests underlying copyright law must be preserved. While unauthorized reproduction of copyrighted works is a valid concern for the recording industry, any measures to curb piracy must also consider the public interest and the limitations on the copyright monopoly—legitimate non-infringing uses of MP3 technology. Copyright law should not function to support outdated business

179. *See* Brown, *supra* note 39.

180. Leonard, *supra* note 12.

181. *See* CONNER-SAX & KROL, *supra* note 4, at 361-62; *see also* Peraino, *supra* note 50.

182. *Weekend Edition-Sunday* (National Public Radio broadcast, Nov. 1, 1998), *available in* 1998 WL 6516736 (information age specialist Rich Dean stating that "so far the music and recording industry has fought just about every innovation, usually because they're concerned about people pirating CDs and tapes.").

183. Leonard, *supra* note 12. The article also notes that "all the music that has ever been released already on compact disc is up for grabs, unprotected and easily transferable," and quotes Michael Robertson of MP3.com as saying, "They are in a pickle.... People are going to have access to these songs if they want them ...."; *see also* Brown, *supra* note 39 (noting that "the real question is whether the record industry will itself try to adapt—and, instead of trying to derail the train, will jump on and take a ride.").

184. Neil Gross, *Target Pirates—Not Technology*, BUS. WK., Nov. 2, 1998, at 40.

models; it should merely support the ability of copyright owners to select their own appropriate business model.

SYMPOSIUM ON INTERNET PRIVACY

"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."
Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890)

Few disagree that the Internet is revolutionizing the way people communicate, conduct business, engage in commerce and express their opinions and feelings. However, the extent of this revolution is limited by Internet users' growing concern for privacy. The Computer and High Technology Law Journal's annual symposium this year addressed the practical implications of the Internet on privacy in a world driven by high technology.

At this well attended event, privacy advocates and leading business representatives explored current privacy expectations and discussed the ways Internet related technology pose threats and present solutions to privacy concerns. Featured speakers included General Counsel of the Federal Trade Commission (FTC) Debra Valentine and California State Senator Debra Bowen as well as industry representatives from eBay, Inc., Fujitsu, and Intel Corporation, and law firm representation from Cooley Godward LLP, Duane Morris & Heckscher LLP, Fenwick & West LLP, Morrison & Foerster LLP, and Wilson Sonsini Goodrich & Rosati. Panel topics included individuals' expectations of privacy, technological threats to privacy and technical solutions, European and U.S. legal solutions, the impact of privacy on ecommerce, and cyber crimes.

We are pleased to present papers authored by three of the symposium speakers, as well as comments authored by one of the speakers. Santa Clara University Professor of Law Dorothy Glancy's essay entitled "Thinking About United States Privacy Law and the Internet" discusses the application of privacy law to Internet activities. In " Privacy on the Internet: The Evolving Legal

Landscape," FTC General Counsel Debra Valentine discusses the FTC's efforts in protecting consumers' privacy on the Internet. Fenwick & West LLP Associate Laurel Jamtgaard discusses the Children's Online Privacy Protection Act in "Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act." Privacy Rights Clearinghouse Director Beth Givens provided her comments on consumers' expectations of privacy protection on the Internet.

We would like to thank our sponsors for their generous contributions to this event: Lexis Publishing, Blakely Sokoloff Taylor & Zafman LLP, Brobeck Phleger & Harrison LLP, Cooley Godward LLP, eBay, Inc., Morrison & Foerster LLP, Wilson Sonsini Goodrich & Rosati, Hoge Fenton Jones & Appel Inc., Finnegan Henderson Farabow Garrett & Dunner LLP, webvan.com, and the American Electronics Association. We would also like to thank all of the Editors and Candidates of the Journal for all of their help, encouragement, and support. Finally, we would like to recognize Assistant Dean of High Technology Ruth Edman, Program Coordinator Cynthia Murphy, and the High Technology Law Program for their co-sponsorship and support to produce this very successful event.

Alison J. Choppelas
Sarah Beth McOwen
Symposium Editors

PRIVACY EXPECTATIONS IN A HIGH TECH WORLD

OPENING PRESENTATION BY BETH GIVENS, PRIVACY RIGHTS CLEARINGHOUSE

Beth Givens[†]

The following comments are based on a speech given by the author on February 11, 2000, at the Santa Clara Computer and High Technology Law Journal's Symposium entitled "Privacy in the New Millennium: A Practical Exploration of the Internet and its Impact on Privacy."

TABLE OF CONTENTS

I. INTRODUCTION

Thank you for the opportunity to participate in this symposium on Internet Privacy. I am honored to be here and to speak on consumers' expectations of privacy protection on the Net.

Let me preface my remarks by providing some background on what the Privacy Rights Clearinghouse does. We were established in 1992 with a grant from the California Public Utilities Commission. Our mission was then, and still is, to increase Californians' awareness of how technology is affecting their lives, and give them practical information on ways to safeguard their privacy.

The definition of privacy on which we have based the PRC is *control*—the ability of individuals to control what is done with their personal information.

In the early days, we operated a toll-free hotline and received as

[†] Director, Privacy Rights Clearinghouse, 1717 Kettner Ave., Suite 105, San Diego, CA 92101, (619) 298-3396 Fax 5681, bgivens@privacyrights.org, www.privacyrights.org.

many as 10,000 calls a year from consumers, handled by myself and law students. When funding declined in 1996, we curtailed the toll-free number but continued the hotline as a toll call. Since then, our web site and electronic mail have become the more common media for fielding consumers' questions and complaints. I estimate that we now interact directly with 3,000-4,000 individuals a year.

The Privacy Rights Clearinghouse is unique among privacy advocacy groups in that we *do* have this *direct* interaction with consumers. I call this our "societal feedback loop." We take what we learn from consumers, analyze it, look for trends and danger points, and feed that information back to legislators, regulators, government officials, industry representatives, other consumer advocates, and people like you interested in policy issues.

II. LEGAL ENVIRONMENT OF PRIVACY PROTECTION

Before discussing consumers' privacy experiences on the Net, I want to provide an overview of the legal environment in the U.S. I believe it explains a great deal about the expectations and experiences of Internet users, not to mention their confusion about their rights to privacy.

The United States has taken a sectoral approach to privacy, enacting laws that apply to specific industries and practices. Examples are:

- the Fair Credit Reporting Act of 1970
- the Privacy Act of 1974
- the Cable Communications Policy Act of 1984
- the Electronic Communications Privacy Act of 1986
- the Video Privacy Protection Act of 1988
- the Telephone Consumer Protection Act of 1991
- the Drivers Privacy Protection Act of 1994
- the Children's Online Privacy Protection Act of 1998.

This patchwork approach is in contrast to the European nations, Canada, Australia, New Zealand, and Hong Kong. These countries have enacted *omnibus* data protection laws covering the full spectrum of uses of personally identifiable information. In some countries, these laws encompass both the private and public sectors. Others at this summit will discuss the European Union's Privacy Directive and the protracted struggle between the EU and the U.S. regarding the adequacy of our privacy protection laws for the purpose of transmitting their citizens' data to the U.S.

From my perspective as a consumer advocate, the sectoral approach has left large gaps where there is little to no protection for individuals.

- There is little regulation of the direct marketing industry's use of personal information, for example, with the limited exception of the telemarketing bill, the Telephone Consumer Protection Act.
- We have no federal law protecting the confidentiality of medical records, although the Department of Health and Human Services has been mandated by a federal law to develop regulations for *electronic* records. These are currently under review and are quite controversial.
- The Cable Act of 1984 includes a fairly good privacy protection section. But the question now is whether it covers data collection by cable companies that offer cable modems and Internet Service Provider services.
- The Fair Credit Reporting Act of 1970 comes the closest to a robust privacy protection law. It enables individuals to have access to their own data profile. They have a right to learn who has accessed their files. And there are restrictions on who can obtain credit reports. Yet this law, too, is limited.
- A more recent example of a robust privacy law is the Children's Online Protection Act of 1998.

III. IMPACTS OF THE SECTORAL APPROACH ON CONSUMERS

What are the impacts on consumers of this sectoral, or patchwork, approach spanning the past 30 years?

- One is consumer confusion. It's a complicated picture. The Privacy Rights Clearinghouse has published 22 guides and a 300-page book telling consumers where they do and do not have protection. Yet we've nowhere near covered the waterfront. I'll revisit the theme of confusion later.
- Another result of the sectoral approach is the absence of cues in the marketplace—little to no disclosure of what is done with personal information and what consumers can do to exert some control. Remember, I am talking about the *off-line* world here. To borrow a term from the European Union, there is little to no *transparency* of information practices.
- A further result of the patchwork approach to U.S. privacy

> protection is that industry has now experienced a long history of having virtually free rein over the use of consumer data. The ability to capture and use information from individuals without getting their permission has become the norm.

Let me bring in the notion of opt-in versus opt-out at this point, because it will no doubt be discussed further at this symposium. *Opt-in* is the standard whereby the entity that gathers information from individuals assumes that it cannot disclose it or use it for secondary purposes without first getting permission from those individuals. *Opt-out* is the situation where the information-gathering entity can further use and disclose the information by default until such time as the individual says "no."

Opt-out has become the norm in the U.S. To illustrate, let me read you a quote from a recent *Wall Street Journal* article in which the Direct Marketing Association laments the decision by the U.S. Supreme Court letting stand the federal Driver's Privacy Protection Act. This law requires states to enable drivers to give consent before their DMV data is used for other purposes. The direct marketing industry has used such data for decades as the source of mailing lists and demographic information.

Here's what DMA said to the *Wall Street Journal* about this law. It is "death to us . . . If you can't use information about a person without permission, that generally means you're not going to have a list of any great substance."[1]

A final result of the patchwork approach to privacy protection is a lack of trust in companies that collect personal information. A 1998 Harris poll on consumer privacy[2] found that:

- Nearly nine in 10 (88%) Americans say they are "concerned about general threats to their privacy."
- Eight in ten (82%) feel they have "lost all control over how companies collect and use their personal information."
- Nearly eight in ten (78%) believe that businesses ask for too much information.
- Three-fourths (78%) say they have "refused to give information to a business . . . because they thought it was too

1. Robert S. Greenberger, *Mass Marketers Say High Court Ruling Will Boost Costs, Mean More Junk Mail*, WALL ST. J., Jan. 18, 2000 at B8.

2. *P&AB Survey Overview: Consensual Marketing Is Coming*, PRIVACY AND AMERICAN BUSINESS, 6:1, at 1 (Jan./Feb. 1999).

personal and not needed." Interestingly, when this question was first asked in 1990, only 42% said they had declined to give such information to a business.

- And, only 43%, or two in five, said they had "exercised an opportunity to opt-out."

IV. CONSUMERS' EXPERIENCES AND EXPECTATIONS REGARDING ON-LINE PRIVACY

Now, we're experiencing the explosion of commerce on the Internet. Web sites are able to capture data from their visitors, and to merge that data with other information. With the exception of the Children's Online Privacy Protection Act and a smattering of state laws regulating spam, or unsolicited electronic mail, there is little regulation of data collection on the Net.

Rather, industry has advocated that they adopt a set of voluntary guidelines based on the opt-out standard. Many commercial web sites, especially those with the highest volume of visitors, have posted notices describing their data collection practices—nearly two-thirds of such websites according to a survey conducted last summer.[3]

Many such sites have joined a web-branding service like TRUSTe or BBBOnline. These programs require that web sites post policies regarding their data collection and use. They also audit their members to evaluate compliance.

It should be noted that over 90% of web sites surveyed by Georgetown University professor Mary Culnan last summer in this study collected data from their users. And less than 10% had privacy policies that contained the all five of the criteria that the Federal Trade Commission had deemed to comprise a proper privacy policy. These criteria are often called "fair information principles." The FTC looked for notice, choice regarding data use, access, security, and enforcement.

The *full* complement of fair information principles include a minimum of eight measures developed by the Organization of Economic Cooperation and Development in 1980. Added to the FTC's four principles are usually collection limitation, accuracy, openness, use limitation, and accountability. The European Union has based its Privacy Directive on the more robust set of fair

3. Mary J. Culnan, *Georgetown Internet Privacy Policy Study* (July 21, 1999) <http://www.msb.edu/faculty/culnanm/gippshome.html> (Mary Culnan is the Project Director).

information principles.

So, what are consumers' experiences on the Net concerning their privacy? I will list several themes that I've observed in talking to consumers and in following news stories about on-line privacy abuses in recent months.

The first theme is the *invisibility* of data capture. We have learned of numerous companies whose web sites have been programmed to track and capture not only surfing patterns, but also information from users' hard drives. For example, the on-line music service RealNetworks secretly compiled information from its users in violation of its own privacy policy. It is a member of TRUSTe.

A result of the invisibility of data capture—or as the EU would describe it, the lack of *transparency* in data collection—is that many consumers lack understanding of what's happening to their data. This situation is similar to the physical world, where, as I mentioned earlier, there are few cues about what is done with personal information.

We have received numerous calls from individuals who say "I want to know what's *out there* about me." When I press them for more details about their concerns, they describe a blurred world of large data bases containing huge amounts of information about them—not altogether untrue. They often are concerned that such unidentified data bases may contain negative information about them, which would explain why they can't find a job.

I think it's significant that these callers often use the same words "out there" and that they have almost no *specific* knowledge of the variety of data files that exist about them, how they're being used, and what limits to usage exist on many of these data bases.

A second theme is the potential *ubiquitousness* of data gathering, and the ability of data from several sources to be merged to create massive electronic dossiers on individuals. We are hearing a great deal these days about the ad-placement network Doubleclick and its ability not only to track users' clickstream as they travel from site to site, but also to be able to link the data gathered on-line with an off-line data source. Doubleclick has merged with Abacus, a company that tracks mail order purchases of about 90 million households. At the time of the merger, the Abacus CEO told MSNBC that "the goal is to have the most complete picture of the consumer you can."

I ask nearly every person who calls our hotline if they have Net access. I want to alert them to our web site and other sites, and to specific fact sheets that can answer their questions. Of those who say

they are *not* Internet users, the majority say, without my prompting them, that they don't want to go on-line because they fear that massive amounts of data will be collected about them.

This observation is borne out in survey data. A 1998 Harris poll found that of those who were not on-line, 70% responded that they would be inclined to start using the Net if "the privacy of [their] personal information and communications would be protected."[4]

A third theme is *invasion.* Web sites can capture and track visitors' clickstream data by placing small text files called "cookies" onto their hard drives. Unless users are savvy enough to set their browsers to notify them about the pending placement of a cookie, it is done without the user's consent, and it's an invisible process. We now hear the word "stalking" being used to describe cookies' tracking capabilities.

A fourth theme is the *fear of harm* befalling Internet users—fear, for example, that their credit card numbers will be stolen. This is not far-fetched given the recent news story of the Russian hacker obtaining over 300,000 account numbers from CD Universe. Many fear that their identities will be stolen, even though this is predominately a low-tech crime. And many fear that the information that is captured will be used for other unrelated purposes.

Although it's not Internet-based, I like to use the example of supermarket buyer's club data to illustrate the potential for secondary uses of personal data. Smith's Foods, a large supermarket chain in the Southwest, has been subpoenaed by the U.S. Drug Enforcement Agency for data on specific customers being investigated for illicit drug manufacture and sale. Were they looking for high-volume purchases of over the counter medications like Sudafed? No, they were interested in learning if these individuals had purchased large quantities of plastic baggies, presumably for packaging the drugs for sale on the street—a most interesting and, to my mind, troubling secondary use of the data given the number of households that probably purchase lots of plastic bags for a variety of uses.

A fifth theme is *confusion* over privacy rights. I have observed that many consumers believe they have far more protection in law than they actually do, whether it's a real world experience they are describing or an on-line experience. They often say to me, "There's a Privacy Act you know, and I have rights."

The Privacy Act these users are referring to is actually rather

4. *New Online Privacy Survey Confirms 1997 P&AB Findings,* PRIVACY AND AMERICAN BUSINESS, 5:1, at 3, 6 (Mar./Apr. 1998).

limited. It addresses what *federal government agencies* can do with personal information. It has no bearing on the private sector. Yet, individuals often think it applies across the board, much like the European countries' data protection laws.

What are the consequences of such experiences by consumers?

- One is reluctance to go on-line, as I mentioned earlier.
- Another is a desire to "mess up the system." Many individuals take great delight in telling me how they falsify information, both on-line and off-line. This is their way of getting even in a marketplace they view as unfair.
- And another is refusal to provide information. In a 1997 Harris survey on Internet privacy, four out of five (79%) respondents who were "asked to provide information when visiting a site declined at some point to provide that information."[5]

V. RECOMMENDATIONS

In conclusion, I have four recommendations for improving privacy protection on the Internet.

The *first* is consumer education. There is a tremendous need for consumers to be knowledgeable about what is happening to them as they surf the Net, to learn the best ways to control the uses of their personal information, and to understand just what legal rights they do and do not have. Such consumer education includes the use of technologies to safeguard their privacy. Consumer education can be conducted by programs like the Privacy Rights Clearinghouse, by government agencies like the Federal Trade Commission and the California Department of Consumer Affairs, and by the commercial web sites themselves. I do not consider the presence of web privacy policies to constitute adequate consumer education. They are often hard to find and difficult to understand.

Ideally, children and teens should be educated in privacy protection strategies in school. This is difficult to do when commercial messages saturate their young lives, showing the Net to be a "cool" and friendly place. Young people are at risk for accepting the present situation as the norm. Canada's requirement that all

5. Mary J. Culnan, *Online Survey Makes Business Case for Privacy*, PRIVACY AND AMERICAN BUSINESS, 4:3, at 11 (1997).

children receive media education in school is certainly laudable.

Second, is the need for a "societal feedback mechanism" whereby individuals' questions and complaints can be heard, analyzed, and ultimately acted upon. Our program is one small example of such a mechanism. The Federal Trade Commission is potentially another. It takes complaints on a much larger scale, but might be constrained by staffing and funding in using its growing database to assess the state of consumer privacy on the Internet.

Third, companies must conduct privacy impact assessments on their products and services in the development stage. How many years was the Pentium III chip in development before it was introduced into the marketplace? The consumer outcry and ensuing back-pedaling by Intel could have been avoided had the privacy implications of the chip's built-in serial number been assessed and dealt with up front. I am heartened to see that several companies have now assembled privacy advisory committees to help guide them in the development of their products.

Fourth, I do believe there is a need for Congress to enact legislation that provides individuals with a baseline of privacy protection on the Net by codifying the fair information principles. The 1998 Harris poll on Internet privacy found that just over half of those surveyed "favor government passing laws to regulate how personal information can be collected and used on the Internet."

There is now a large body of evidence that industry self regulation is not working. While nearly two-thirds of the largest web sites have privacy policies, the vast majority of them are simply disclosure statements providing just two of the fair information principles, notice and opt-out. Most policies omit the other principles such as access, accuracy, security, collection limitation, and accountability. Furthermore, we are learning that many companies are not in compliance with their existing policies. A study was recently released by the California Healthcare Foundation[6] showing that many health-related web sites collect information from their visitors and disclose it to third party marketers contrary to their stated policies.

I look forward to the upcoming panels where issues such as industry self regulation and technology solutions are explored in depth.

---

6. Janlori Goldman, Zoe Hudson and Richard M. Smith, *Report on the Privacy Policies of Health Care Web Sites* (Feb. 2000) <http://ehealth.chcf.org/priv_pol3/index_show.cfm?doc_id=33>.

With that I conclude my remarks. Thank you.

AT THE INTERSECTION OF VISIBLE AND INVISIBLE WORLDS: UNITED STATES PRIVACY LAW AND THE INTERNET

Professor Dorothy Glancy[†]

TABLE OF CONTENTS

I. INTRODUCTION

"You already have zero privacy—get over it," warned Scott McNealy, chief executive of Sun Microsystems at the launch of his company's Jini consumer networking software.[1] In fact, laws protecting privacy are everywhere in the United States. These privacy laws intersect with the Internet in more ways than even Mr. McNealy might imagine. The problem is that thinking about how United States privacy law interacts with the Internet can be perplexing. Just as the British poet, Stephen Spender wondered at "understanding the intersection of visible with invisible worlds," observers of privacy and the Internet can be bewildered by the complexity of the intersecting elements. Of course, unlike Spender's image, aspects of invisibility and visibility, concreteness and abstraction, are woven into both the Internet and privacy laws.

The purpose of this essay is to consider some characteristics of

† Professor of Law, Santa Clara University School of Law; B.A. Wellesley College; J.D. Harvard Law School. This essay is based on remarks prepared for the symposium, *Privacy in the Next Millennium*, February 11-12, 2000 at Santa Clara University.

1. John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, Mar. 3, 1999, at A1.

United States privacy law that contribute to the obscurity of many intersections between the Internet and privacy law. This discussion is not an exhaustive catalogue of all of the ways in which United States privacy law may apply to Internet activities. Nor is it intended to be an evaluation of the effectiveness of this privacy law. Rather, the point here is to explore why the application of privacy law to the Internet is a matter of considerable complexity and some uncertainty. The focus is on certain characteristics of privacy law that can mislead even very smart people into believing that privacy is not here.

Both the Internet and United States privacy law operate in varied ways across many dimensions. Just as the Internet is an interconnection of digital networks that operates in multiple ways to communicate data and other information worldwide, United States privacy law embraces many types of laws that protect and vindicate individual self-determination with regard to personal activities, private decisions, and personal information about an individual.[2] With regard to the Internet, a varied assortment of privacy laws function in different ways to protect and to vindicate individual control over personal activities, decisions, and information. The complexities of the potential interactions between privacy law and the Internet may be difficult to visualize. But it is a mistake to count privacy, and the laws which protect it, as zero.

II. THREE CHARACTERISTICS OF UNITED STATES PRIVACY LAW

Three main characteristics of United States privacy law help to explain why it can be difficult to understand how privacy law intersects with the Internet. First, United States privacy law is diverse. Second, United States privacy law is decentralized. Third, United States privacy law is dynamic. As privacy law has evolved over the past century or so, these characteristics have resulted in a myriad of specific privacy laws applicable in the United States. Only a few of the details of these privacy laws can be noted here.

Consider an average Internet user, Irene.[3] During a typical week,

---

2. Warren & Brandeis first described the right to privacy as a right to an "inviolate personality." *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890). The article argued that: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others ... fix[ing] the limits of the publicity which shall be given to them." *Id.* at 198.

3. See results of a recent study by the Stanford Institute for the Quantitative Study of Society. Norman H Nie & Lutz Erbing, *Internet and Society: A Preliminary Report* (visited Feb. 18, 2000) <http://www.stanford.edu/group/siqss>. The survey was based on a nationwide

Irene is on-line for five hours or so, reading and sending e-mail to friends and business associates, doing research and writing reports. Sometimes Irene participates in Internet auctions or purchases books or airline tickets from Internet companies. She subscribes to a couple of Usenet groups and occasionally visits chat rooms and on-line forums. Irene probably believes that her Internet activities are private. But she is most likely unaware of the multitude of privacy laws applicable to her activities on the Internet. Although these privacy laws may not perfectly protect Irene's on-line privacy,[4] if Irene were aware of the many ways in which privacy laws affect her on-line, she would be amazed.[5]

A. Diverse

Understanding United States privacy law begins with the recognition that privacy law is not an "it." Instead, United States privacy law is a very diverse collection of many different types of privacy laws. The tendency of these privacy laws to focus on specific, even narrow, privacy concerns or contexts has generated widespread criticism of privacy laws in the United States as "piecemeal" or fragmented.[6] A number of years ago a federal appeals court judge described United States privacy law as like a "haystack in a hurricane."[7] In an opinion for the United States Supreme Court, Chief Justice Rehnquist criticized privacy as "defying categorical description."[8] Even the distinguished privacy advocate, Arthur R.

---

random sample of 4,113 individuals over the age of 18 in 2,689 households. Over a third (36%) of those responding reported being on-line at least five hours each week. Almost half of the respondents reported Internet use of between one and five hours per week. *See* John Markoff, *A Newer, Lonelier Crowd Emerges in Internet Study*, N.Y. TIMES, Feb. 16, 2000, at A1 fig.

4. Indeed, aspects of privacy law may well be antiquated, out of sync with modern life, not to mention Internet technologies. Since most privacy law was not designed with the Internet in mind, loopholes and misfits are to be expected. However, privacy law's many imperfections are not the focus of this discussion. Rather the point here is to demonstrate that, although a great deal of privacy law does apply to Irene's on-line activities, understanding that privacy law can be difficult.

5. Professor Lawrence Lessig has ably addressed different, but no less intriguing, issues regarding the architecture of the Internet and whether the Internet is being designed and built with acceptable respect for privacy values in mind. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999). Chapter 11 discusses the value of privacy and the importance of building it into the architecture of the Internet. *See id.* at 142-63.

6. Almost every imaginable imagery of a heterogeneous mixture has been used to describe United States privacy law. Many of these metaphors seem to be based on food—from hodgepodge (stew) to succotash (mixed vegetables).

7. Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481, 485 (3d Cir. 1956), *cert. denied* 351 U.S. 926 (1956).

8. Paul v. Davis, 424 U.S. 693, 713 (1976).

Miller, described United States privacy law as "a thing of threads and patches."[9] And yet the very diversity that makes privacy law seem difficult to pin down also contributes to its vitality and makes its application to the Internet interesting.

Three aspects of the diversity of United States privacy laws are particularly important: (i) the tendency of modern privacy law to divide into at least two main branches of privacy interests: privacy concerns about autonomy and privacy concerns about personal information; (ii) the variety of different types of privacy laws; and (iii) the specific, context-dependent nature of many privacy laws. These characteristics of privacy law account for much of the internal diversity and complexity of United States privacy law.

1. Autonomy and Personal Information

As United States privacy law evolved over the past century, two general branches developed. These two branches reflect what are perceived to be different types of privacy concerns: On the one hand, privacy law is concerned about an individual's autonomous control over personal activities and decisions. On the other hand, privacy law is also concerned about an individual's control over personal information about that individual.[10] For example, the California Supreme Court has described the guarantee of an "inalienable right to privacy" in the California constitution as divided into two separate areas of privacy interests: "(1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference ('autonomy privacy')."[11] Depending on the category into which a particular privacy case fits, a different privacy analysis applies.

Although often treated as separate categories, autonomy privacy and informational privacy are in fact intimately intertwined, particularly when privacy law intersects with the Internet. For example, assume that our average Internet user, Irene, objects to

9. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 169 (1971).

10. In *Whalen v. Roe*, 429 U.S. 589, 598-99 (1977), Justice Stevens noted that: "The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."

11. Hill v. National Collegiate Athletic Ass'n, 7 Cal. 4th 1, 35, 865 P.2d 633, 654, 26 Cal. Rptr. 2d 834, 856 (1994); *see also* discussion in *American Academy of Pediatrics v. Lungren*, 16 Cal. 4th 307, 332, 940 P.2d 797, 812, 66 Cal. Rptr. 2d 210, 225 (1997) (plurality opinion).

surreptitious electronic surveillance of her Internet activities through the collection of personal information about her on-line activities. Such an objection is partly classified as a concern about autonomy privacy—her ability to control her life and her choices about how to live that life. This privacy concern is about her "right to be let alone," frequently associated with the autonomy right to privacy.[12] At the same time, Irene is also concerned about whether personal information about her is stored, manipulated, connected up with other information or disseminated to others. For example, Irene may well be concerned about a marketing company's collecting information about the web sites she visits, about the company's manipulating this information into an "Irene" on-line profile, about the company's connecting that profile with other information (such as her address and telephone number), and also about the company's selling the whole consumer picture of Irene to a marketing firm. These informational privacy concerns are, of course, interrelated with her autonomy privacy concerns. Internet users, such as Irene, object to collection of information about their on-line activities both because such surveillance interferes with their individual autonomy and because they have an informational privacy interest in controlling the use of such information. Nevertheless, United States privacy law often places these concerns in separate categories and applies different analysis to each of them.

Because the Internet is an information network, most Internet observers look at Internet activities as involving primarily informational privacy concerns about controlling the collection, storage, manipulation, and dissemination of personal information. For example, Irene is concerned about unauthorized disclosure of her credit card numbers or her bank account balance. But such concerns are only part of the picture. In fact, for Irene and other Internet users, autonomy privacy interests in preventing the collection of such information in the first place may well be of even greater practical importance. After all, personal information that is not collected cannot be stored, manipulated or disclosed.

Autonomy privacy interests are often associated with such issues as decisions regarding contraception[13] and abortion.[14] But autonomy

12. *See* Warren & Brandeis, *supra* note 2, at 195. The notion of a "right to be let alone" is usually attributed to Judge Thomas Cooley, who described it as "[t]he right to one's person may be said to be a right of complete immunity: the right to be let alone." THOMAS M. COOLEY, COOLEY ON TORTS 29 (1879).

13. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965).

14. *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973).

privacy also extends to an individual's self-determination regarding who will have how much access to that individual.[15] In the Internet context, Irene's autonomy privacy concerns include her ability to control whether or not her purchases of various types of goods and services from Internet sites are compiled into her consumer profile, since that profile is likely to be a "stand-in" or alter-ego for her with regard to future transactions. Autonomy privacy concerns also arise when censors or snoopers interfere with Irene's choices to send and to receive information over the Internet.[16] Surreptitious surveillance of Irene's Internet activities, for example through "cookies" or by creation of an on-line profile of her browsing habits, also raise autonomy concerns about her privacy on the Internet. Another example of autonomy privacy is Irene's choice to visit web sites anonymously. She might, for example, decide to participate in a Usenet group for expectant mothers under a pseudonym without revealing her actual identity. Irene might also choose to interact with the Internet through a persona or avatar. Her screen name might be "Inez" or "Ike" in a chat room, for example. Such autonomous self-redefinition illustrates a slightly different, and controversial, form of autonomy privacy, sometimes called anonymity[17]or pseudonymity. Although privacy tort actions have for a long time protected an individual's autonomy privacy right to self-definition and redefinition,[18] the extent to which such autonomy privacy concerns

---

15. The initial argument for recognizing a right of privacy in the United States defined privacy as based on the principle of "an inviolate personality" associated with "the right to be let alone." Warren & Brandeis, *supra* note 2, at 205; *see also* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 21-28 (1979).

16. *See* Stanley v. Georgia, 394 U.S. 557 (1969). In this case involving the seizure of obscene film from a person's home, Justice Marshall insisted that the

> Right to receive information and ideas, regardless of their social worth, is fundamental to our free society .... [T]he right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy .... If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.

Id. at 564-65.

17. *See generally* Anne W. Branscomb, *Anonymity, Autonomy, Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1995).

18. *See, e.g.*, Melvin v. Reid, 112 Cal. App. 285, 297 P. 91 (1931). This damage action for invasion of privacy was brought in the 1930s by a reformed prostitute against film makers who made a movie, "The Red Kimono," in which they used both the facts of her former life as a prostitute and her maiden name. The court found that, having reformed and redefined herself as a respectable married woman, she had a recognizable cause of action based on "the right to live one's life in seclusion, without being subjected to unwarranted and undesirable publicity. In

can or should be translated into privacy law applicable to the Internet remains controversial.[19]

2. Reasonable Expectations of Privacy

Legal protections for both autonomy privacy interests and informational privacy interests often depend in part on whether expectations of privacy are considered reasonable in a particular setting.[20] For example, legal protection for Irene's privacy is likely to depend in part on whether she reasonably expects privacy when she accesses the Internet. Since Internet users, such as Irene, would be reluctant to log onto the Internet if they could not reasonably expect at least some degree of privacy with regard to their on-line activities, they appear to have at least some reasonable expectation of privacy on the Internet. Assurances of privacy protection by e-commerce vendors[21] and Internet service providers[22] demonstrate that the

---

short, it is the right to be let alone." *Id.* at 289, 297 P. at 92 (1931).

19. Objections to Internet anonymity are typically based on concerns about the potential for untraceable criminal activity such as money laundering, misappropriation of intellectual property, or drug trafficking. *See* United States Department of Justice, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, (Mar. 2000) <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm> (Report of the President's Working Group on Unlawful Conduct on the Internet).

20. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967). Katz was a wiretapping case involving Fourth Amendment objections to interception of Katz's telephone calls from a public telephone booth. The majority opinion is famous for its ruling that the privacy protections in the Fourteenth Amendment protect "people and not simply 'areas.'" *Id.* at 353. Justice Harlan stated in his concurring opinion that whether there was a search for Fourth Amendment purposes depended on two factors, "first, whether the person involved exhibited an actual, subjective, expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'." *Id.* at 361 (Harlan, J., concurring).

21. For example, American Express begins its Internet Privacy Statement with the assertion: "Protecting your privacy is important to us." *American Express Customer Internet Privacy Statement* (visited Apr. 2, 2000) <http://home3.americanexpress.com/corp/consumerinfo/privacy/privacystatement.asp>. The "Lycos Privacy Policy" page features not only a statement about Lycos's subscription to the TRUSTe privacy protection program but also "Our Privacy Vow." *See Lycos Privacy Page* (visited Apr. 2, 2000) <http://www.lycos.com/privacy/>. Unfortunately the content of this "privacy vow" seems to have more to do with collecting information than with respecting privacy. The vow states:

> Our goal at Lycos is to be 'Your Personal Internet Guide' by providing you with the information and services that are most relevant to you. To achieve this goal, we need to collect information to understand what differentiates you from each of our millions of other unique users. We collect this information in two ways.

Id.

The bottom line of the Lycos Privacy Policy, its last element, is entitled "Delete/Delist," and states, "[i]t is not currently possible for a Lycos customer to delete his or her information from the database." *Id.* A personal request to be removed from the database will, however, be honored, according to the Lycos Privacy Policy. *See id.*

commercial side of the Internet recognizes that respect for privacy is a significant expectation of Internet users.

Although the Internet may appear to some as a wide open and not very private environment, not every bit of digital data on the Internet is open to anyone who knows how to access it.[23] For example, encryption, fire walls and other data security techniques can make certain Internet information inaccessible as a practical matter. Moreover, simply declaring the Internet non-private does not necessarily make it so;[24] nor does such a declaration eliminate reasonable privacy expectations on the part of Internet users. In reality, Internet users, such as Irene, reasonably expect some degree of privacy on the Internet, both because they are repeatedly assured that their privacy is being respected, and because privacy laws of many types protect and vindicate privacy rights with regard to both their autonomy and their control over personal information.

3. Types of Privacy Laws

Many types of privacy laws, both civil and criminal, protect and vindicate privacy interests in the United States. Although mostly developed before the Internet, these various types of privacy laws can apply to on-line activities of Internet users. A detailed description of all of these types of privacy laws is beyond the scope of this essay. But it is useful to highlight some of the major types including constitutional law, common law, statutory law, regulatory law, as well as self-regulatory measures.

---

22. For example, see AOL's "Privacy Policy," which states "America Online, Inc. is strongly committed to protecting the privacy of consumers of its interactive products and services." *AOL.com, Privacy Policy* (visited Apr. 2, 2000) <http:\\www.aol.com/info/privacy.html>.

23. Lawrence Lessig has argued that the Internet can and should be even better organized and constructed to respect privacy. *See* LESSIG, *supra* note 5, at 142-63 (discussing the issue of privacy in Chapter 11).

24. The United States Supreme Court frowned on what the Court called "conditioning" expectations of privacy in *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (finding no search when the government used a pen register to record numbers dialed from a telephone). In a footnote, the Court noted that the government cannot eliminate legitimate expectations of privacy by suddenly

> [A]nnounc[ing] on nationwide television that all homes henceforth would be subject to warrantless entry [so that] individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects .... In such circumstances, where an individual's subjective expectations had be 'conditioned' by [extraneous] influences ... a normative inquiry would be proper.

Id. at 740 n.5.

As an example, consider the privacy laws applicable to electronic surveillance of Irene's Internet activities of the complex layers of different types of privacy laws. Irene is logged on to the Internet at home through a modem. Assume that Gill, a law enforcement officer, intercepts Irene's Internet communications, without a warrant or intercept order, and records Irene's e-mail messages and Internet transactions without her knowledge or consent. Gill's invasion of Irene's privacy is illegal under federal statutes prohibiting wiretapping without a warrant, as well as under the Fourth Amendment to the United States Constitution and other civil and criminal laws regulating electronic surveillance by government agencies and agents.[25] Assume further that Paul, a private investigator, similarly taps and records Irene's on-line communications and transactions. Paul's invasion of Irene's Internet privacy would subject Paul to both civil and criminal penalties under different provisions of federal electronic surveillance statutes, as well as under privacy laws of most states.[26] As will be discussed further with regard to the decentralized nature of privacy law, a combination of both federal and state privacy laws, including both civil and criminal statutes and state common law, would make electronic surveillance of Irene's Internet communications illegal on many levels.

Of the various types of privacy laws, those relating to constitutional privacy rights are probably the most controversial.[27] According to Justice William O. Douglas's expansive view of constitutional rights to privacy, the penumbras of several provisions

25. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (1994); Privacy Protection Act, 42 U.S.C. §§ 2000aa to 2000aa-12 (1994); McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998). Gill may also be in violation of state constitutional provisions and statutes. *See, e.g.*, CAL. CONST. art. 1, § 13; CAL. PENAL CODE § 630 (West 1999).

26. Federal statutes include the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (1994) and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1994). An example of a state criminal statue penalizing wiretapping is CAL. PENAL CODE § 631 (West 1999). The common law tort of intrusion, discussed *infra* at notes 36, 47-55, may also provide a basis for damage liability.

27. The reasons for the controversial status of federal constitutional privacy rights are many. *See* Dorothy J. Glancy, *Douglas's Right of Privacy: A Response to His Critics*, *in* "HE SHALL NOT PASS THIS WAY AGAIN:" THE LEGACY OF JUSTICE WILLIAM O. DOUGLAS 155 (Stephen L. Wasby ed., 1990). In the first place, the United States Constitution does not contain the word "privacy." Moreover, there is a broad range of many types of implicit constitutional privacy rights—from rights to receive information to rights to make decisions about procreation. Some of these privacy rights involve matters of deep-seated social and religious disagreement. For a critical discussion of Douglas' expansive view of the constitutional right of privacy see William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, 23 U. KAN. L. REV. 21 (1974).

of Bill of Rights, including the First, Third, Fourth, Fifth, and Ninth Amendments, and the Fourteenth Amendment as it applies to the states, all protect privacy.[28] These federal constitutional privacy rights are safeguarded against governmental action interfering with an individual's privacy. Most of them focus on the autonomy branch of privacy law. For example, Gill's warrantless electronic surveillance of Irene's Internet activities would violate her Fourth Amendment right against unreasonable searches.[29] In addition, government interference with Irene's rights to unhindered communication with others, and against surveillance of her reading habits would most likely be unconstitutional under the First Amendment. Regarding government collection of personal information about Irene's Internet activities and storing it in a database, the United States Supreme Court has suggested that, government mandated databases of personal information where the information is not lawfully collected nor adequately safeguarded, may violate federal constitutional privacy guarantees.[30]

Most state constitutions contain search and seizure provisions similar to those in the federal constitution.[31] A few state constitutions also contain provisions explicitly protecting privacy. For example, the California Constitution expressly guarantees "an inalienable right to privacy."[32] Moreover, California's state constitutional privacy provision applies broadly to prohibit interference with privacy both by governmental and by private-sector invaders.[33]

As a result, if Irene were on-line in California, her Internet activities would be protected under California's constitution against both misuse of personal information about her and interferences with her autonomy. This state constitutional privacy protection would apply to invasions of privacy both by government agents, such as

28. *See, e.g.*, Griswold v. State of Connecticut, 381 U.S. 479 (1965) (holding unconstitutional a Connecticut criminal statute which penalized the distribution of birth control information or devices to married persons).

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

30. *See* Whalen v. Roe, 429 U.S. 589, 605 (1977). Justice Stevens' majority opinion included "[a] final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Id. Cf.* Nixon v. Administrator of General Services, 433 U.S. 425 (1977) (concerning former president's constitutional privacy interest in avoiding disclosure of personal matters).

31. *See, e.g.*, CAL. CONST. art. 1, § 13.

32. *Id.* § 1.

33. *See* Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1976).

Gill, and by private investigators, such as Paul.

A second type of privacy law is part of the common law of torts. The origins of common law protection for privacy in the United States date back to a famous 1890 law review article, *The Right to Privacy*, largely written by Louis Brandeis, later a United States Supreme Court Justice.[34] Almost all states now allow such damage actions for invasion of privacy. In fact, the common law of most states recognizes four different privacy torts. The Restatement (Second) of Torts Sections 652A—652I, adopted by the American Law Institute in 1977 provides a conventional description of the four privacy torts:[35]

- Unreasonable intrusion upon seclusion (commonly referred to as "Intrusion")[36]
- Appropriation of another's name or likeness (commonly referred to as "Appropriation")[37]
- Unreasonable Publicity given to another's private life (commonly referred to as "Private Facts")[38]
- Publicity unreasonably placing another person in a false light (commonly referred to as "False Light")[39]

These four privacy torts are "personal" in the sense that only the living individual whose privacy has been invaded has the right to bring a lawsuit based on them.[40] Privacy tort actions are also generally limited by absolute and conditional privileges similar to those applicable in defamation actions, such as consent and First Amendment protection for freedom of expression.[41] In most cases involving these privacy torts, liability requires the privacy invasion to have been unreasonable.

---

34. Warren & Brandeis, *supra* note 2. The article described invasion of privacy as interference with an individual's "inviolate personality" and argued that the common law should allow damage actions to redress and punish invasions of privacy. *See id.* at 198, 205. *See generally* Glancy, *supra* note 15.

35. RESTATEMENT (SECOND) OF TORTS §§ 652A-I (1977). The Restatement (Second) of Torts [hereinafter "Restatement"] categories reflect an analysis of privacy cases by William Prosser, who was the Reporter for that Restatement. *See generally* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

36. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

37. *Id.* § 652C. Sometimes this privacy tort is described as vindicating a right to publicity.

38. *Id.* § 652D.

39. *Id.* § 652E.

40. *See id.* § 652I. In some states, statutes provide for the survival of privacy tort causes of action. *See, e.g.*, CAL. CIV. CODE § 3344.1 (West 2000).

41. *See* RESTATEMENT (SECOND) OF TORTS §§ 652F-652G (1977).

So far, only a few reported decisions have applied the Restatement's categories of common law privacy torts to the Internet, and only in regards to the Fourth and Fifth Amendments.[42] In the context of computer networks, reported decisions include *Wood v. National Computer Systems, Inc.*[43] and *Morrow v. II Morrow, Inc.*[44] In both of these cases, summary judgment for defendants was held appropriate because the allegedly privacy-invading material was not sufficiently published to the public at large, but rather was disclosed within a restricted network. Although distribution on a local area network (LAN) might not satisfy the "publication" required for liability under the privacy torts involving publicity, Internet distribution of information does seem to provide sufficient publicity for the appropriation, private facts and false light privacy torts. For example, in *Michaels v. Internet Entertainment Group, Inc.*, the Federal District Court granted a preliminary injunction preventing an adult entertainment Internet content provider from distributing over the Internet a videotape of celebrity plaintiffs, Bret Michaels and Pamela Anderson Lee, engaged in sexual activity.[45]

It is interesting to consider how each of the common law privacy torts might apply to an Internet user such as Irene, who is accessing the Internet from her home.[46] For the purposes of the intrusion privacy tort, whether or not Irene can be said to have seclusion on the Internet depends in part on the extent to which the Internet can be considered a private place. Generally, the Restatement's concept of seclusion depends on whether a plaintiff's expectations of privacy are reasonable in that particular setting.[47] Public opinion polls about privacy concerns with regard to Internet activities seem to suggest that at least some on-line activities, such as those involving healthcare information or personal financial information communicated in e-

42. *See, e.g.*, Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997); McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).

43. 643 F. Supp. 1093, 1098 (W.D. Ark. 1986) (teacher's competency examination report mistakenly sent to another teacher did not constitute public disclosure of private facts).

44. 139 Or. App. 212, 911 P.2d 964 (Or. App. 1996) (false-light invasion of privacy action against employer who posted critical evaluation of employee on hard drive accessible company-wide was not established because employer did not distribute personal information to public generally).

45. 5 F. Supp. 2d 823 (C.D. Cal. 1998). Although the preliminary injunction was based on both invasion of privacy and copyright infringement, the court specifically found that the plaintiffs were likely to prevail on privacy claims based on appropriation and publicity given to private life. *See id.* at 840.

46. Different privacy law analysis would apply if Irene were on-line in her employer's offices.

47. *See* discussion *supra* notes 20-24.

commerce transactions, are considered reasonably secluded.[48] The commentary to Restatement Section 652B suggests that protected seclusion covers "private concerns" such as an individual's "private and personal mail, searching his safe or his wallet, examining his private bank account."[49] It seems unlikely that the Internet venue for such matters as personal mail or personal bank account records would render such information any less secluded. The illustration to the Restatement section 652B that focuses on repeated annoying promotional telephone calls to a person's home despite repeated requests to desist seems to suggest that personally targeted "push" technology might constitute an unreasonable intrusion on seclusion.[50] Even if the Internet were considered a public place, the intrusion privacy tort[51] may still apply in cases of intrusion into "a private seclusion that the plaintiff has thrown about his person or affairs."[52] The comment to this part of the Restatement notes that: "Even in a public place . . . there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters."[53] There are often issues regarding consent in intrusion cases.[54] But the privacy tort that vindicates seclusion generally requires that the determination of the individual be respected with regard to matters that the particular individual considers personal.[55]

Irene's status as an Internet user does not affect her general privacy right to prevent having her name or likeness appropriated for the use or benefit of someone else.[56] Most of the decisional law regarding tort liability for invasion of privacy by appropriation involves commercial use, such as advertising. When commercial use

48. *See, e.g.*, Mary J. Culnan, GEORGETOWN INTERNET PRIVACY POLICY STUDY: REPORT TO THE FEDERAL TRADE COMMISSION (Mary J. Culnan, study director, 1999); Janlori Goldman et al., PRIVACY: REPORT ON THE PRIVACY POLICIES AND PRACTICES OF HEALTH WEB SITES (Feb. 2000) <http://ehealth.chcf.org/priv_pol3/index_show.cfm?doc_id=333>. As noted, *supra* notes 21-22, privacy policies, vows and assurances by Internet companies reinforce expectations of seclusion. Images of locks visually enhance such an expectation of privacy.

49. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

50. *Id.* at illus. 5.

51. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977)..

52. *Id.* at cmt. c.

53. *Id.*

54. *See* RESTATEMENT (SECOND) OF TORTS § 652F cmt. b. (1977).

55. *Cf.* Massachusetts v. Source One Assoc., Inc., No. CIV.A.98-0507-H, 1999 WL 975120 (Mass. Super. Oct 12, 1999) (unauthorized acquisition of personal financial information).

56. *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977).

of a person's name or likeness takes place on-line, the liability analysis developed in cases involving other commercial media would apply. For example, using Irene's picture on BrowserCo's web site as the image of a "happy BrowserCo user" without her consent would probably be actionable. In addition, as commentary to the Restatement suggests, there may be liability for appropriation of Irene's personality even in the absence of commercial use "and even though the benefit sought to be obtained is not a pecuniary one."[57] According to the Restatement, passing oneself off as someone else or "otherwise seek[ing] to obtain for [one]self the values or benefits of the plaintiff's name or identity," is actionable.[58] If another person uses Irene's identity to gain benefits, such as credit from an Internet retailer, or to gain access to valuable Internet services to which Irene is a subscriber, that person may be liable for invading Irene's privacy for appropriating her name or likeness.

There are a number of unanswered questions regarding application of the appropriation privacy tort in the Internet context. For example, whether Irene's "personal image" in the form of her on-line profile of browsing habits and purchasing patterns constitutes a likeness of her for the purposes of the appropriation privacy tort remains an open question.[59] The privacy rights of an Internet user, such as Irene, to consent or not to consent to transfers of her on-line profile by Internet retailers or marketing firms is central to the debate over opt-in, as opposed to opt-out, consumer control over information reflecting a person's Internet use. Whether Internet users in the United States must be asked to consent to each appropriation of information about their on-line activities (opt-in) or, rather, whether Internet users have implicitly consented to general use of digitized profiles of their Internet activities so that each Internet user must expressly withdraw consent to sale of such information (opt-out), remains a very contentious privacy issue.[60] In privacy tort cases,

57. *Id.* at cmt. b.

58. *Id.* at cmt. c. Whether it would be actionable under the common law appropriation privacy tort to use a famous, or infamous, screen name or Internet persona to advertise an Internet security service is an intriguing matter which has yet to be litigated. Logically if the name refers to an individual person, the common law tort should apply. Alternative grounds for liability in such cases might be based on copyright or trademark, if the persona or screen name were copyrighted or trademarked.

59. *See* Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977). In this case the United States Supreme Court upheld privacy tort liability for appropriation despite First Amendment protection of freedom of expression, when a television station broadcasted the performer's entire act as a human cannon ball. *Id.* at 575.

60. For example, Financial Services Legislation of 1999, Pub. L. No. 106-102, § 502, 113

consent is often construed narrowly so that a deliberate decision to opt-in would ordinarily be required.

Both private facts and false light privacy torts require publicity in the form of widespread dissemination that goes beyond mere "disclosure" or "publication" as these terms are understood in the law of defamation. With regard to publicity over the Internet, the *Michaels* case, *supra*, is an example of an actionable invasion of privacy for publicity regarding private facts over the Internet. Posting Irene's tax returns on an Internet bulletin board or surreptitiously webcasting digital pictures of Irene privately celebrating a family birthday would probably also constitute tortious public disclosure of private facts, if done without her consent. If digital pictures of Irene's family celebration were accompanied by misleading references, such as to "the secret problem of inebriation at home," common law tort liability for false light invasion of privacy might arise. Even certain kinds of Internet spoofing by posting slanted information regarding an individual, for example by describing Irene, who is a gregarious person with a happy family and many friends, as a "lonely woman seeking affection on-line," might give rise to false light privacy tort liability.[61]

Privacy statutes are even more numerous and varied than the common law privacy tort actions. Some state privacy statutes enact particular versions of the privacy torts. For example, in some states statutory rights of publicity authorize causes of action against exploitation of celebrity personalities.[62] These statutory publicity rights are similar to privacy rights vindicated by the appropriation tort, but often provide more extensive privacy protection.[63] Other statutes have enacted new forms of privacy rights against invasions of privacy, such as cyberstalking, that were arguably not actionable

---

Stat. 1338, 1437 (Nov. 12, 1999) adopted an opt-out approach with regard to transfer of information within a financial institution, but an opt-in approach with regard to disclosures outside of that financial institution. Given the conglomerate nature of many financial institutions, which may now include insurance, investments, credit reporting and other services under the 1999 Financial Services Legislation, the opt-out provisions applicable to transfers within a financial institution, may result in a much wider presumption of consent to transfer than is realistic.

61. *See* Cantrell v. Forest City Publ'g Co., 419 U.S. 245 (1974). *Cf.* Time, Inc. v. Hill, 385 U.S. 374 (1967).

62. *See* CAL. CIV. CODE § 3344 (West 1997). According to the Ninth Circuit, these statutory rights are in addition to the common law tort privacy rights. *See* Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988).

63. *See* CAL. CIV. CODE § 3344.1 (West 2000) which provides for survival of the statutory publicity rights of deceased persons.

under the common law.[64] Another example is California Civil Code section 1708.8(b), regarding constructive invasion of privacy, which penalizes use of visual or auditory devices to capture images of personal or familial activities.[65] Many privacy statutes focus on particular types of information, such as consumer credit records protected under the Fair Credit Reporting Act,[66] or Drivers License Records,[67] or on particular databases, such as federal agencies' systems of records containing personal information, protected under the Federal Privacy Act.[68] These privacy statutes are not specifically directed at Internet activities, but rather would apply to the Internet when the specified personal information or privacy invading conduct occurs on the Internet.

A few statutes target Internet invasions of privacy. For example, the Children's Online Privacy Protection Act[69] is directed at protecting the privacy rights of children who access the Internet. This statute would protect the privacy of Irene's eight and ten-year old children, James and Jennifer, who are each on-line about an hour a day. Another example of a type of state statute directed at Internet invasions of privacy is the cyberstalking statute such as California's amendments to its anti-stalking statute noted above.[70] If Irene were on-line in California, for example, the cyberstalking statute would make it illegal for someone to follow her about by shadowing her activities on the web and sending her threatening e-mail messages.

In addition to privacy statutes, privacy laws also include agency

---

64. *See* CAL. CIV. CODE § 1708.7 (West 2000) (establishing liability for stalking, including threats communicated by means of electronic communication devices).

65. *Id.* § 1708.8(b). This statute states:

> A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.

Id.

66. 15 U.S.C. §§ 1681-1681t (1994); *see also In re* TransUnion Corp., No. 9255 (FTC Mar. 29, 2000) < http://www.ftc.gov/os/2000/03/transunionrestay.htm>.

67. The Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994); *see also* Reno v. Condon, 120 S. Ct. 666 (2000) (upholding the Act's validity).

68. 5 U.S.C. § 552a (1994).

69. 15 U.S.C.A. §§ 6501-6506 (West 1999).

70. *See* CAL. CIV. CODE § 1708.7 (West 2000).

regulations that provide privacy protection.[71] For example, each federal agency subject to the Federal Privacy Act is required to publish regulations with regard to the nature of that agency's systems of records containing personal information about individuals.[72] These Privacy Act regulations provide Irene both a way to discover which federal agencies maintain databases containing personal information about her and a process for accessing that information.[73] Other examples of regulatory privacy law affecting the Internet are the Federal Trade Commission's proposed regulations implementing the Children's Online Privacy Protection Act[74] and the Department of Health and Human Services proposed regulations regarding medical records.[75]

In addition to constitutional, common law, statutory and regulatory privacy laws, non-governmental self-regulatory measures can also be the bases for legal privacy rights for Internet users such as Irene. Theses self-regulatory measures commonly take the form of a company's own privacy principles. Sometimes companies adopt codes of fair information practices put forward by trade associations. For example, Irene might encounter Amazon.com's privacy principles[76] or those of American Express[77] when she buys books or airline tickets over the Internet. These on-line privacy measures may be given legal effect to the extent that non-compliance would constitute a deceptive trade practice. For example, Internet retailers often make privacy promises to induce customers, such as Irene, to engage in electronic commerce with these companies. If an Internet retailer promises not to disclose Irene's Internet purchasing records to any other company, and then turns around and sells Irene's purchasing history to a direct marketing firm, the Internet retailer may be liable under deceptive trade practices laws. The Federal Trade Commission has taken unfair trade practices actions against companies that have announced privacy principles to attract

71. *See, e.g.,* 34 C.F.R. § 99.1-.67 (2000) (Department of Education regulations implementing the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1994)).

72. 5 U.S.C. § 552a(e)(4), (f) (1994).

73. *Id.* at (d).

74. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888 (1999) (to be codified at 16 C.F.R. pt. 312) (proposed Apr. 27, 1999).

75. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (1999) (to be codified at 45 C.F.R. pts. 160-64) (proposed Nov. 3, 1999).

76. *See Amazon.com: Your Privacy* (visited Mar. 5, 2000) <http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html/>.

77. *See American Express Customer Internet Privacy Statement, supra* note 21.

customers, but then failed to abide by their avowed privacy protection promises.[78] Such enforcement under deceptive trade practices laws means that if Internet companies falsely represent to Irene that they will protect her privacy, they may face potential legal liability for interfering with the privacy protection promised in gaining her business.

4. Context-dependent

Particular on-the-web applications of privacy laws frequently depend on the contexts of alleged invasions of privacy. This context-dependency is at least partly explained by the way privacy law has evolved over the past century or so, often in reaction to particular invasions of privacy. For example, when Brandeis first argued that the common law should recognize a damage action for invasion of privacy, he pointed to the notorious case of Marion Manola, an actress photographed in tights against her will.[79] More recently, the use of motor vehicle license records by murderers of young women has led to the enactment of statutes restricting the availability of such records.[80] Although a few privacy laws apply broadly to a general form of invasion of privacy, such as electronic surveillance,[81] privacy laws typically focus on a particular situation or type of personal information. For example, the federal Video Privacy Protection Act provides for the privacy protection of video rental records.[51] This statute was enacted into federal law after the records of Judge Robert Bork's videotape rentals surfaced in Senate hearings regarding his nomination to the United States Supreme Court.[83] Because privacy law has characteristically evolved by solving a particular type of

78. *See In re* Geocities, Inc., No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999) (ordering Geocities to cease deceptive trade practices in the form of misrepresentations regarding the use and collection of personal information).

79. *See* Warren & Brandeis, *supra* note 2, at 195. The lawsuit, Manola v. Stevens & Meyers, is discussed in Dorothy J. Glancy, *Privacy and the Other Miss M*, 10 N. ILL. U. L. REV. 401, 402-19 (1990).

80. The Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994), was prompted by the 1989 murder of actress Rebecca Schaeffer, star of the hit television series, "My Sister Sam." *See* 139 CONG. REC. S15745-01, *515762 (1993) (statement of Sen. Boxer); *see also* Ellen Barry, *Killer's Dreams Bared on the Internet N.H. Man Took to Web to Boast and To Stalk*, BOSTON GLOBE, Nov. 29, 1999, at B1; *Killer Plotted Murder Through Internet*, S.F. CHRON., Nov. 30, 1999, at A12.

81. *See* discussion *supra* notes 26-27.

82. 18 U.S.C. § 2710 (1994).

83. *See* S. REP. NO. 100-599, at 5-6 (1988); *see also House OKs Video Privacy Protection Bill*, L.A. TIMES, Oct. 20, 1988, at I2; ETHAN BRONNER, BATTLE FOR JUSTICE: HOW THE BORK NOMINATION SHOOK AMERICA 274 (1989).

privacy problem or by reacting to a notorious invasion of privacy, or by protecting a particular type of personal information, it is not surprising that context plays an important role in the diversity of privacy law.

For the most part, the privacy laws applicable to Irene's on-line activities were not designed for the Internet context, but rather can be applied to her Internet activities by extrapolation from other settings. In considering extrapolation of privacy laws to the Internet, two contextual factors are particularly noteworthy. First, different privacy laws will apply depending on whether the invasion of privacy involves collection of personal information or manipulation of personal information or dissemination of personal information. Second, different privacy laws will apply depending on whether privacy is invaded by the government or by the private sector.

Some privacy laws concentrate on controlling collection of personal information. For example, the constitution and federal statutes restrict unauthorized electronic surveillance of Irene's on-line activities without a warrant or intercept order.[84] The intrusion privacy tort also provides a basis for imposing liability for improper collection of such personal information. And yet the collection of information about Irene's Internet browsing remains controversial. Marketing companies maintain that placing cookies in Irene's browser or identification numbers in her microprocessor has nothing to do with Irene's privacy, because the information collected does not personally identify Irene. Rather, the information collected only identifies hardware or software, not any identified person who may be manipulating the hardware or software. The potential that records of Internet activities can be combined with other information to identify Irene as the user of the identified microprocessor or software cookie has, however, raised serious privacy concerns.[85] Whether such information is personal to Irene at the time it is collected, or only potentially personally identifiable after it is connected to other information, is among the privacy questions posed by the nearly infinitely replicable, manipulable and aggregateable qualities of

84. *See* discussion *supra* notes 25-26; *see also supra* notes 82-83.

85. For example, plans by DoubleClick to integrate its web-browsing records with the consumer database of Abacus, a direct marketing company acquired by DoubleClick raised a storm of protest, first from privacy advocates and later from Wall Street. *See* Jeri Clausing, *Privacy Adovcates Fault New DoubleClick Service*, N.Y. TIMES, Feb. 15, 2000, at C2; *Privacy on the Internet*, N.Y. TIMES, Feb. 22, 2000, at A26; Bob Tedeschi, *In a Shift, DoubleClick Puts Off Its Plan for Wider Use of the Personal Data of Internet Consumers*, N.Y. TIMES, Mar. 3, 2000, at C5.

digitized information. What is certain is that the Internet's global network magnifies the consequences for individual privacy when a vast range of such digitized information is collected about people and their on-line activities.

With regard to aggregation of personal information, the 1999 Financial Services Legislation permits considerable manipulation and aggregation of personal information within a financial institution.[86] As financial institutions become global providers of insurance, stock-trading, savings accounts and direct marketing, in addition to retail banking, there will be enhanced opportunities for widespread sharing and manipulation of personal data among the many subsidiaries and affiliates of modern financial institutions. It is interesting to contrast this permissive approach in the financial services legislation, allowing widespread sharing of personal information about customers within a financial institution, with the approach in the Privacy Act, which restricts the transfer of an individual's personal information among federal agencies.[87]

When dissemination of personal information is the context of privacy concerns, different privacy laws apply. Examples include the privacy torts of appropriation, private facts and false light as well as the Fair Credit Reporting Act. Different approaches to legal protection against improper dissemination of personal information are characteristic of these privacy laws. For example, the Fair Credit Reporting Act prohibits dissemination of Irene's credit history without her consent for all but a few restricted purposes.[88] The disclosure of private facts privacy tort, on the other hand, provides a basis for Irene to bring suit for damages against an Internet company from which she purchased exotic lingerie, if that company were to publicly post the details of her purchases on its web site.[89]

Another contextual factor that causes different privacy laws to apply is whether interference with privacy has been perpetrated by the government or by the private sector. It is interesting to note that Brandeis's initial discussion of privacy law was focused on non-governmental interferences with privacy, mostly by newspapers.[90] Later, Brandeis came to see government as posing an even greater

86. *See* Financial Services Legislation of 1999, Pub. L. No. 106-102, § 502, 113 Stat. 1338, 1437 (Nov. 12, 1999).

87. *See* 5 U.S.C. § 552a (1994).

88. 15 U.S.C. § 1681b-1681c (1994).

89. *See* discussion *supra* notes 38, 45. Common law tort liability is also possible under appropriation and false light privacy theories for Internet postings of personal information.

90. *See* Glancy, *supra* note 15, at 8-17.

danger to individual privacy:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping.... Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law;.... To declare that the government may commit crimes in order to secure the conviction of a private criminal would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.[91]

Justice William O. Douglas agreed with Brandeis that the government's threat to privacy was much more serious than that posed by the private sector.[92]

Although concerns about government interference with privacy remain important,[93] at the turn of the twenty-first century, the focus of privacy concerns seems to have turned increasingly toward worries about invasion of privacy by private-sector hackers and crackers and telemarketers. Thomas Friedman calls this the "little brother" problem,[94] as distinguished from the problem of omnipresent government surveillance symbolized by "Big Brother" in George Orwell's novel, *1984*.[95] Internet users seem to be particularly concerned about private-sector collectors, manipulators and sellers of personal information in what is now a globalized marketplace. Privacy law has always been responsive when new threats to privacy are identified. The focus of primary concerns about government invasions of privacy, such as those associated with Watergate, seem to shifting toward enhanced concern about invasions of privacy by the private sector, such as those associated with disclosures of credit card numbers from Internet sites. Underlying concerns about protecting individual privacy from being overwhelmed by society, whether in the form of big government or in the form of big business, remains a strong force in American law.

---

91. Olmstead v. United States, 277 U.S. 438, 474-85 (1928) (Brandeis, J., dissenting). Eventually the United States Supreme Court agreed with Brandeis and reversed Olmstead. *See* Katz v. United States, 389 U.S. 347 (1967).

92. *See* WILLIAM O. DOUGLAS, THE RIGHT OF THE PEOPLE 123-24 (1958); *see also* Wyman v. James, 400 U.S. 309, 335 (1971) (Douglas, J., dissenting); Dorothy J. Glancy, *Getting Government Off the Backs of People*, 21 SANTA CLARA L. REV. 1047, 1050-51 (1981).

93. *See The Searchable Soul*, HARPER'S MAG., Jan. 1, 2000, at 57.

94. *See* Thomas L. Friedman, *Little Brother*, N.Y. TIMES, Sept. 26, 1999, Sec. 4 at 17; Thomas L. Friedman, *The Hackers' Lessons*, N.Y. TIMES, Feb. 15, 2000, at A31.

95. GEORGE ORWELL, 1984 (1950).

B. Decentralized

The decentralized nature of United States privacy law further complicates understanding the intersections of privacy law with the Internet. There are not only diverse types of privacy laws operating in many different contexts, but also many different sources of these laws. Federal law and state law provide the two primary sources of privacy law in the United States. In addition, as noted earlier, sometimes these state and federal privacy laws interact with private-sector representations regarding privacy policies and industry privacy standards. As a result, if Internet users such as Irene were suddenly to see the operation of the privacy laws potentially applicable to their Internet activities, they would see these privacy laws coming from several directions at once.

The decentralized pattern of United States privacy law is in marked contrast to the more centralized approach taken in Europe, associated with the 1995 European Union Data Protection Directive.[96] The overall purpose of the European Data Protection Directive is to harmonize within the European Union the law which applies to processing personal information relating to an identified or identifiable natural person[97] Under the Data Protection Directive, every member state in the European Union is required to adopt strict privacy laws providing privacy rights at minimum levels described in the directive. Such a centralized "harmonization" contrasts with the deliberately decentralized "cacophony" of United States privacy law.[98]

Federalism is the primary reason why United States privacy law has generally avoided the centralized one-size-fits-all approach exemplified by the European Data Protection Directive. Indeed, reflecting federalism, United States privacy law mixes both federal and state laws, and also accommodates a divergent pattern of state privacy laws that often vary considerably from state to state. In another context, Justice Brandeis insisted that it is important for states

96. *See* DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (October 24, 1995) <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html>. Effective October 25, 1998, the Directive is subject to continuing refinement.

97. *See id.* at arts. 2-3.

98. The European Data Protection Directive can have practical consequences with regard to Internet activities involving personal information if these activities take place in part in Europe. Difficult and still unresolved, issues with regard to jurisdiction over Internet activities to make it hard to predict which nation's privacy law will apply in any given circumstance involving transnational flows of personally identifiable data.

to be able to experiment with social and economic legislation. He noted that "it is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments."[99] Although Brandeis was not discussing privacy law in *New State Ice Co. v. Liebmann*, one of the most interesting social and economic areas in which extensive experimentation has taken place across the states, as well as between the states and the federal government, is with regard to privacy laws.

A good example of the decentralized pattern of federal and state privacy law is the complex layering of federal and state privacy laws regarding electronic surveillance discussed earlier in this essay.[100] Initially based primarily on federal constitutional and statutory law, these electronic surveillance laws now include the variety of both state and federal privacy laws that are applicable to electronic surveillance of Internet communications. Consider how both federal and state laws protect the privacy of Irene's Internet communications. Recall that Gill is a federal law enforcement official who has tapped Irene's modem line to intercept her Internet communications without a warrant or intercept order and that Gill's invasion of Irene's privacy is illegal under federal law.[101] Recall also that interception of Irene's Internet communications by a private investigator, Paul, would violate different provisions of federal wiretap statutes, as well as provisions of state law in most states.[102] However, in some states, such non-governmental recording of Irene's Internet communications through use of an extension telephone on Irene's modem line would be illegal; but in many other states such interception would not be considered an invasion of privacy. For example, if Irene were on-line in California, use of the extension line would violate California's highly restrictive electronic surveillance laws.[103] But if Irene were on-line in New

99. New State Ice Co. v. Liebmann, 285 U.S. 262, 311(1932) (Brandeis, J., dissenting).

100. *See supra* text accompanying notes 25-26.

101. *See* U.S. CONST. amend. IV; Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (1994); Privacy Protection Act, 42 U.S.C. § 2000aa to 2000aa-12 (1994); McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998). If Gill were a state law enforcement official, he might also be in violation of state constitutional provisions and statutes. *See, e.g.*, CAL. CONST. art. 1, § 13; CAL. PENAL CODE § 630 (West 1999).

102. *See, e.g.*, Biton v. Menda, 796 F. Supp. 631 (D.P.R. 1992). The Federal Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (1994), does not preempt state statutes which provide more protection to the privacy of electronic communications. *See* 18 U.S.C. § 2516(2) (1994).

103. *See* CAL. CONST. art. 1, § 1; CAL. PENAL CODE § 630-37.2 (West 1999); Ribas v. Clark, 38 Cal. 3d 355, 696 P.2d 637, 212 Cal. Rptr. 143 (1985).

Hampshire, that state's more permissive electronic eavesdropping laws would permit use of the extension telephone line to record Irene's Internet transmissions.[104]

Although, privacy protection in the United States typically comes from a mixture of federal and state privacy laws, an interesting, and rare, exception to the decentralized pattern of federal and state privacy laws is the law that applies to the privacy of consumer credit records under the Federal Fair Credit Reporting Act.[105] With certain limited exceptions, only federal law applies with regard to matters covered by the Fair Credit Reporting Act.[106] Aside from the Fair Credit Reporting Act, state privacy laws are generally not preempted by federal law. For example, the 1999 Financial Services Legislation expressly allows states to adopt more stringent privacy protections.[107] So far, Internet users have not expressed interest in a unified federal privacy law that would preempt state experimentation with divergent approaches to privacy protection. Rather, Brandeis's notion of benign variation among state privacy laws, as well as between federal privacy laws and state privacy law seems likely to continue to be the preferred pattern of privacy laws in the United States.

C. Dynamic

Compounding the diversity and decentralization of United States privacy laws, is the remarkable dynamism of privacy law in the United States. From its inception in the nineteenth century, privacy law has evolved in response to new challenges to the privacy interests of individuals, particularly challenges posed by new technologies. This dynamic quality of privacy law is evident as old privacy laws confront new challenges posed by the Internet. Indeed, part of the original argument for recognition of the right to privacy in the United States was based on the need to respond to societal and technological change:

> Political, social and economic changes entail the recognition of new rights . . . Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing to the individual what Judge Cooley

104. *See* State v. Telles, 139 N.H. 344, 653 A.2d 554 (1995).

105. 15 U.S.C. § 1681-1681t (1994).

106. *Id.*

107. *See* Financial Services Legislation of 1999, Pub. L. No. 106-102, § 507(b), 113 Stat. 1338, 1442 (Nov.12, 1999).

> calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'[108]

Among the privacy threatening technologies that worried Warren and Brandeis 1890 were the flash camera, plate glass, the telephone and telegraph.[109] Later, in his famous dissenting opinion in *Olmstead*, Brandeis expressed concern that "Discovery and invention have made it possible for the government by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[110] He speculated that

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[111]

Had Brandeis imagined the Internet, he most likely would have predicted, and urged, further development of privacy law.

Contemporary society's voyeuristic interest in prying into the details of personal life, evident in such aspects of popular culture as talk radio and shock broadcasting,[112] pose a counter force against development of laws more protective of privacy.[113] Internet webcasting of activities including sexual intercourse, childbirth, working on homework and all sorts of other ordinary life activities, from the trivial to the profane, brings private life onto the web—on web cam, on-line, available virtually all of the time. Such challenges to privacy are not new. Even in 1890, Warren and Brandeis expressed outrage over the destructive impact of widespread

---

108. Warren & Brandeis, *supra* note 2, at 193, 195.

109. *See* Glancy, *supra* note 15, at 8.

110. Olmstead v. United States (Brandeis, J., dissenting), 277 U.S. 438, 473 (1928).

111. *Id.* at 474.

112. Typical examples are television's "The Jerry Springer Show," the film, "The Truman Show" and "Big Brother," which broadcasts the real lives of individuals over television in Holland and Germany.

113. Judge Richard Posner has described this voyeurism as the interest in prying, which weighs against the interest in privacy. *See* Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394-97 (1978).

publication of the details of private life: "To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers."[114] The Internet's proven capacity for even wider circulation of ever more personal and private information would undoubtedly have greatly troubled Warren and Brandeis, who counted the devaluation of private life through widespread disclosure as among the important policy reasons for legally protecting the right to privacy.

As the Internet itself rapidly evolves, new privacy challenges are certain. For example, a recent research report predicts that there will be more than 1.4 billion Internet participants world-wide by 2004.[115] What is perhaps even more remarkable is that the report predicts that by 2004 a majority of Internet participants will access the Internet over mobile terminals—both handheld and in vehicles. An estimated 670 million people will access the web through fixed or "wired" platforms. But 750 million people will access the web over wireless modems, PDAs such as Palm Pilots and Psions, and Internet access built into vehicles.[116] The suggestion is that the World Wide Web may well be rapidly transforming into a Wireless World Wide Web. As this transformation in Internet usage takes place, new privacy law issues will undoubtedly arise. These new privacy law issues not only include intensified privacy concerns with regard to the security of wireless Internet communications. They also will reflect privacy concerns about an individual's control over information that pinpoints an individual's geographical location as she accesses various sites on the Internet from changing locations.

III. CONCLUSION

Despite Scott McNealy's pessimistic views, privacy is unlikely to wither away in the United States. If the past is any guide to the future of privacy law, the American public is unlikely to "get over"

---

114. Warren & Brandeis, *supra* note 2, at 196. The article decried the publication and circulation of personal information as "potent for evil" and explained:

> It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.

Id.

115. *See* THE ARC GROUP, WIRELESS INTERNET: APPLICATIONS, TECHNOLOGY & PLAYER STRATEGIES (1999). The contents of the report are also available at <http://www.the-arc-group.com/reports/wireless_internet/toc_wi/htm>.

116. *See id.*

privacy anytime soon. The privacy laws discussed in this essay already affect the Internet in remarkable ways. The future is likely to bring to bear even more privacy laws. These privacy laws may well remain invisible to most people. But there will be privacy laws intersecting with the Internet in more ways that even sophisticated Internet users may imagine. The wide spectrum of participants in the February 2000 symposium on Privacy in the Next Millennium sponsored by the Santa Clara Computer and High Technology Law Journal presented a clear demonstration that the interaction between privacy law and the Internet remains a matter of significant concern to those who think, write legislate and regulate about privacy in the twenty-first century.

BIG BIRD MEETS BIG BROTHER: A LOOK AT THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Laurel Jamtgaard[†]

TABLE OF CONTENTS

On April 21, 2000 the Children's Online Privacy Protection Act[1] ("COPPA") will go into effect and companies operating on the Internet will no longer be able to ignore the growing number of children flocking to hang out on-line. Although the intent of COPPA is to curb the activities of those who take advantage of children on-line, it will require a broad range of on-line companies to alter their web sites and information practices. Fortunately for such companies, the attention that they pay to complying with COPPA may help them comply with other privacy related regulations that are on the way.

Some view COPPA as a continuation of the U.S. "piece meal" approach to privacy regulation but others see it as evidence of a new tide of general privacy regulation in the United States. Until now, the U.S. approach to privacy has combined (a) a set of narrowly defined

[†] Associate at Fenwick & West LLP, Palo Alto, CA; A.B. Stanford; J.D. UC Berkeley, Boalt Hall. I thank the student organizers of the Santa Clara Privacy Symposium for giving me the opportunity to participate in the symposium and the incentive to write this piece. The opinions expressed herein are my own and are not necessarily the opinion of Fenwick & West LLP or any of the clients that I may advise.

1. 15 U.S.C.A. §§ 6501-6506 (West Supp. 1999).

laws focused upon specific types of bad acts,[2] with (b) a reliance upon industry "self-regulation" to develop general standards and build a consensus for privacy in the on-line world.[3] But, as consumers take to the Internet with enthusiasm and learn that everything they buy, view, or "click on" is recorded in a database and can be indexed and queried in innumerable ways, the willingness to rely on self-regulation is waning. Increasingly, federal and state regulators are stepping into the privacy arena with calls for legislation to increase consumers' control of their information.

This is indeed a busy time for privacy regulation in the United States. In addition to COPPA, we are seeing increased monitoring of privacy concerns by the Federal Trade Commission ("FTC").[4] The privacy protection provisions of the Financial Services Act of 1999 are not yet in effect but will entwine many on-line companies in the Act's regulation of data sharing among "financial institutions."[5] The Supreme Court recently affirmed the Driver's Privacy Protection Act[6] and in it the principle that Congress may regulate personal information held by state agencies. The White House and Congress

---

2. *See, e.g.*, the Video Privacy Protection Act, 18 U.S.C.A. § 2710 (West Supp. 1999) (adopted in reaction to the public disclosure of video tape rental records of Robert Bork when he was a nominee to the U.S. Supreme Court); the Cable Communications Policy Act, 47 U.S.C.A. § 551 (West 1991 & Supp. 1999); the Electronic Communications Privacy Act of 1986, 18 U.S.C.A. § 2701-2711(West Supp. 1999); and the Drivers Privacy Protection Act of 1994, 18 U.S.C. § 2721 (West Supp. 1999).

3. *See, e.g.*, Self Regulation and Privacy Online: A Report to Congress, Federal Trade Commission, July 1999. The Report can be found at <http://www.ftc.gov/os/1999/9907/privacy99.pdf>.

4. The FTC is not only leading the implementation of COPPA and the Financial Services Act privacy regulations, it has also launched investigations against individual companies based upon privacy concerns and, recently, has announced an investigation into the privacy practices of the on-line health care industry. *See* Keith Perine, *FTC Probes Health Site Privacy*, The Standard (Feb. 18, 2000) <http://www.thestandard.com/article/display/0,1151,11120,00.html?nl=dnt>.

5. *See* 12 C.F.R. § 225.28(b)(9)-(14) (1999) (explaining that among other things "financial institution" shall include companies providing certain types of management consulting services; companies issuing consumer-type payment instruments; and companies offering data processing services related to financial data); *see also* Bank Holding Company Act of 1956, 12 U.S.C. § 1841 (1994). The FTC has published proposed rules and the comment period to respond will close March 31, 2000 (Mar. 1, 2000) <http://www.ftc.gov/os/2000/02/65FR11173.pdf> (to be codified at 16 C.F.R § 313 "Privacy of Consumer Financial Information, Proposed Rule").

6. *See* Condon v. Reno, No. 98-1464, 1999 S. Ct. Cornell (Jan. 12, 2000), *rev'g* 155 F.3d 453 (holding that the Driver's Privacy Protection Act of 1994 (DPPA or "Act"), 18 U.S.C.A. §§ 2721-2725 (West Supp. 1999), did not violate the Constitutionally protected principle of federalism). The decision can be found at <http://supct.law.cornell.edu/supct/html/98-1464.ZO.html>.

are pushing toward medical privacy protection regulations.[7] And the Commerce Department, after lengthy negotiations, has reached a tentative agreement with the Europeans for "safe harbors" to enable multi-national companies to comply with the broad European consumer privacy regulations.[8] All this, combined with the flurry of class action suits against various software and on-line advertising companies, means that the risks to a U.S. company operating on the Internet of not defining, disclosing, and internalizing a reasonable privacy protection policy are very real and are growing each day.

Although this article will focus on COPPA and the issues that it raises for companies dealing with consumers on-line, it will hopefully serve a broader purpose because companies that proactively work to comply with COPPA will find that they are a step ahead as other privacy regulations arrive. In Part I, I provide a basic overview of the Children's Online Privacy Protection Act. In Part II, I discuss several issues that companies will face with regard to COPPA including (a) who in the company should be involved with decision-making about privacy, (b) whether the scope of COPPA reaches a company's on-line practices, and, (c) assuming that the company will be affected by COPPA, some options for complying with the new rule.

I. ABOUT COPPA–BACKGROUND, STATUS AND BASIC PROVISIONS

Congress passed the Children's Online Privacy Protection Act in October 1998 at the end of a session in an omnibus bill and without much fanfare or public controversy. The bill addressed the emotionally charged concern that commercial web site operators were targeting children (those under 13) and collecting personal information from them without notice to their parents. In November 1999, the FTC issued the rule to implement COPPA, known as the Children's Online Privacy Protection Rule (the "Rule").[9] The Rule goes into effect April 21, 2000.

---

7. See the recently proposed rules announced October 9, 1999, by the Department of Health and Human Services. Electronic Privacy Information Center, Wash. D.C., *HHS Medical Privacy Regulations* (last modified Oct. 29, 1999) <http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html>.

8. *See* DRAFT INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE, (Mar. 14, 2000) <http://www.ita.doc.gov/td/ecom/RedlinedPrinciples31600.htm> and the Press Release accompanying the Draft (Mar. 14, 2000) <http://204.193.246.62/public.nsf/docs/8B7937D138B4F735852568A30053A385>.

9. 16 C.F.R. § 312 (1999). The FTC provided detailed analysis in connection with the Rule.

A central provision of COPPA provides:

> It shall be unlawful for any operator of a website or online service directed to children [age 12 or younger], or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part.[10]

An "operator" is a person or company that operates a web site or on-line service for commercial purposes and that collects personal information about users.[11] This includes e-commerce sites offering products or services for sale from the web. One important exception to note for many organizations that interact with children is that this definition of operator excludes non-profit web sites and personal home pages with "guest books."[12]

"Personal Information" is information that could enable someone to be contacted on-line or in the real world. It includes first and last name, physical address, e-mail address, instant message identifier, phone number or photographs.[13] Anonymous data such as traffic data collected using cookies will be considered "personal information" if it is tied to personally identifiable data.[14] For example, if a web site operator associates data about what pages a visitor has viewed with a unique identifier that can be used to contact the person through e-mail, a physical address or even an on-line message name, the page view data will be considered "personal information."

There are five key requirements of COPPA: (1) Notice; (2) Parental Consent; (3) Parental Review; (4) Limits on the Use of Games and Prizes; and (5) Security.

With the notice requirement, an operator of an on-line service directed to children must provide notice about what information it collects from the children that use its service, how it uses the information it collects and to whom, if anyone, it discloses that information.[15] The notice must be placed in a "clear and prominent" manner on the home page of the site, or area directed to children, and on any page where personal information is collected.[16]

---

10. *Id.* § 312.3.
11. *See id.* § 312.2.
12. *See id.*
13. *See id.*
14. *See id.*
15. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4(b) (1999).
16. *Id.*

The parental consent requirement is perhaps the most onerous. It states: "Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent."[17] Web sites seeking consent must employ reasonable efforts to ensure that the consent is genuine taking into account available technology. I discuss this consent requirement further in Part II.

An operator must provide a means for a parent to review information that has been collected and a means for the parent to contact the operator to prohibit further use or maintenance of the child's personal information.[18] The FTC does not go so far as to require that an operator enable a parent to *alter* the data provided by the child, but encourages companies to enable that option.[19] Except as limited by section 312.7 of the Rule discussed below, an operator may refuse to continue to provide its service to a child if the parent has prohibited further use of the personal information.[20]

In order to avoid enabling improper access to a child's personal information, the process for enabling a parent to review a child's information must itself involve some reasonable procedure of verification of the parent without unduly burdening the parent.[21] This identification process is not required for an operator who provides the requesting adult only with the *types* of information collected about a child. But the identification process is required before revealing the child's personal information to the requesting adult.

Web sites that direct games and prizes to children in an effort to get targeting information about them should take careful note of section 312.7. It states that "[a]n operator is prohibited from conditioning a child's participation in a game, the offering of a prize of another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity."[22] The FTC provided very few comments about this section, thus web sites are likely to have questions about what information would be considered "reasonably necessary."

Under section 312.8, operators must protect the confidentiality,

17. *Id.* § 312.5.

18. *See id.* § 312.6.

19. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59904 (1999) (to be codified at 16 C.F.R. pt. 312).

20. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.6(c) (1999).

21. *See id.* § 312.6(a); *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59903.

22. 16 C.F.R. § 312.7 (1999).

security, and integrity of personal information collected from children. Most web sites are increasing security procedures at a rapid pace to keep up with the danger of hackers and system outages. Section 312.8 reiterates the importance of establishing and maintaining internal and external security measures including firewalls, information deletion, limits on employee access to data, and careful screening of third parties to whom such information is disclosed.[23]

II. INTERNALIZING COPPA–QUESTIONS AND ISSUES

A. Who in the Company Should be Involved?

Before discussing the legal issues surrounding COPPA, it is important to highlight corporate awareness as the most important goal for a company subject to COPPA. The first thing a company should do is decide which internal employees and outside advisors should be involved in evaluating the company's approach to user privacy. For many small start-up web companies, this is fairly straight-forward. Usually, whoever is in control of the web site's content (often a marketing manager) will contact the company's outside counsel to discuss the company's compliance with COPPA. As questions arise, the company's information technology or computer services director may get involved to advise on how the solution may be implemented using the company's existing database applications and user registration processes.

For a large company, determining who should be involved can be daunting. There may be hundreds of people within the corporation who have direct design responsibilities for some portion of the web site or network of related web sites and who may have access to the information collected from the web site or from customers via e-mail. Large portals or media sites will have a tough job getting a privacy message out to all the employees who have a need to know. To address this problem, many companies have created whole departments focused on setting and implementing privacy, data management, and data integrity policies. And, job postings for "Chief Privacy Officer" are on the rise.

A review of a company's privacy policy and its exposure under COPPA will involve marketing, business development, legal, and

23. *See id.* § 312.8; *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59906.

information technology issues. Companies that want to get ahead of the privacy wave should plan to involve voices from each of these areas in planning their approach to user privacy. Companies with international operations will have already begun this privacy review as a result of privacy regulation in other parts of the world. With COPPA in place, many more U.S. companies now have a clear incentive to do so.

B. Scope of the Rule

For companies evaluating COPPA's impact on their business, the threshold question is whether the company's activities even come within the scope of the regulation. With COPPA, this can be a difficult determination to make. COPPA only applies to: (1) web sites directed/targeted to children under 13 years of age; (2) "general audience" web sites that have a portion of the site targeted to children; and (3) general audience web sites that have "actual knowledge" that they are dealing with a child or that a child is disclosing personal information through the web site.[24]

1. Sites Targeted to Children

If a web site is "targeted to children," the rules of COPPA apply across the board to the site's information collection practices. Thus, in order for the site to collect any personal information from any visitors, even adults, the site must comply with the provisions of COPPA and seek some sort of adult verification.

A likely result of COPPA will be that sites clearly targeted to young children under 13 will not collect any information that would require obtaining parental consent. Sites targeted to teenagers, or that have content that is attractive to kids of all ages, will be in an uncertain position because they may be unsure whether the FTC or a court will consider them to be "targeted to children."

Under COPPA, determining whether a site is "targeted to children" will involve consideration of "subject matter, visual or audio content, age of models, language or other characteristics of the web site or on-line service, as well as whether advertising promoting or appearing on the web site or on-line service is directed to children."[25] The use of animated characters may increase the

24. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.3 (1999); *see also* § 312.2 (definition of "website or online service directed to children").

25. *Id.* § 312.2.

likelihood that the site will be considered targeted to children.[26] The FTC will consider empirical evidence regarding audience composition and evidence about the "intended audience."[27] Unfortunately for some web sites this "guidance" leaves a lot of room for interpretation and, as discussed below, may chill the information practices and services of web sites unsure of where they stand.

Because the FTC has said that it will look at the intent of the web site operator, I have encouraged clients to review their web sites, focusing on areas and features that may unintentionally seem to be directed to children. Companies should take the time to make a conscious decision about directing or not directing content to children if they have any desire to gather personal information from visitors to those areas of their site.

The growing on-line advertising industry led by the much publicized DoubleClick will need to be cautious about serving ads to sites or areas of sites directed to children. In the FTC's Statement accompanying the Rule, the FTC stated that if companies that serve banner advertisements "collect personal information directly from children who click on ads placed on web sites or on-line services directed to children, then they will be considered operators who must comply with the Act, unless one of the exceptions applies."[28] The FTC added in a footnote that: "It may be appropriate for such companies to provide a joint notice with the operator of the host website."[29] With the pace of the industry, it is difficult to ascertain what level of information is being collected by such companies, but, if they are either collecting personally identifiable information from kids who click on ads, or if they are able to tie anonymous cookie data they collect with personally identifiable information from another source, they will need to comply with the Rule.

In fact, COPPA may impact many players in the on-line advertising industry. Banner advertisements increasingly employ data entry windows. That data may be sent directly to one or more of several entities including the company that is advertising its products or services, an advertising agency, and advertising serving company, or the web site providing the banner space itself. If the web site that offers a banner window "knows" that the user viewing the web page

26. *See id.*

27. *Id.*

28. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59891 (1999) (to be codified at 16 C.F.R. pt. 312).

29. *Id.* at 59892 n.57.

is a child, will that knowledge be imputed to the advertising agency or the ad serving company? Perhaps banner ads will have to have their own privacy policies?

These questions are complicated further when one realizes that an ad serving company is often not in a direct contractual relationship with the web sites to which it serves ads, but rather it may have an intermediary agreement with an advertising agency. This lack of contractual privity between the ad serving company and the web site may either protect the ad serving company from knowledge or may just make it more important for them to monitor where they are serving ads. As the contracting party, it may bring the advertising agencies into COPPA's reach even if they do not place cookies, collect the information or serve the ads.

2. General Audience Sites

The primary choices available to a general audience web site under COPPA are to: (1) stop collecting subscriber information (not attractive); (2) refrain from asking for age; (3) prohibit membership by those under 13; and/or (4) seek adult verification for those who self-identify as under 13. For general audience sites, the choice between options 2, 3 and 4 or some combination thereof, will come down to a cost benefit analysis and depend largely on the make up of the user base, the relative dependence on age-targeted advertising, and the types of services offered.

Even if the web site is attractive to those from age 10 to 20, the 10 to 12-year-olds may be asked to stand on the sideline in order for the web site to avoid the additional burden of "knowing" that a user is a child. (Of course, many of the kids will probably just "sneak in" by registering as 15-year-olds.) If a site knows that a member is a child, requests for additional information in the future may require another round of obtaining parental consent.

COPPA applies to "disclosures" of personal information by children as well.[30] Thus, even general audience sites that do not collect personally identifying information but offer chat services with "screen names" can get in sticky territory if they monitor the chat rooms.[31] If a user identifies herself as a child and submits a message containing her personal contact information and the "monitor" sees it, then the monitor will need to delete the personal contact information from the posting in order for the site to be able to say that it did not

30. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (1999).

31. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59889.

"collect" the information. Sites that *want* to monitor their chat rooms to prevent them from degrading into worthless banter and sex talk will need to educate the employees and agents who do the "monitoring" about COPPA rules.

The potential liability for allowing children to disclose personal information is in sharp contrast to the broad shield against liability for defamation claims that on-line service providers now wield thanks to § 230 of the Communications Decency Act of 1996[32] and its broad interpretation in recent case law.[33] Neither Congress nor the courts have offered on-line service providers safe harbors from contributory liability for invasions of privacy by their users. COPPA's limited safety zones may be the guide for future regulation in this area.

3. Web Sites in the Grey Area

Until benchmark cases are addressed in the higher courts, many sites that have a significant percentage of users under age 13 will be unsure whether their policy of "prohibiting membership by those under 13" or seeking permission for those who self-identify as under 13 will suffice. If they are considered "directed to children," statements meant to dissuade participation by children will not matter – all users will need to demonstrate that they are an adult or, if a child, that they have their parental consent before the site can collect information from them (subject to the exceptions discussed below).

In particular, web sites directed to teenagers may not be able to tell whether they will be considered "directed to children." I have advised some clients to analyze their membership database to record current usage statistics by age in order to support their claim that the site is not "directed to children." When they stop collecting age information in order to avoid "actual knowledge," they will render themselves less able to demonstrate the actual age statistics of their users.

Consider web sites focused upon video games. The audience age range will be wide but concentrated in the teens and twenties. If a gaming site has an audience of 10 to 12-year-olds that makes up 5% of its total audience, would that make the web site "targeted to children?" Such a label seems unlikely, but the 5% could represent thousands of kids. Would a court or the FTC be swayed by evidence that the 5% of members of a service who are children equals fifty

32. 47 U.S.C.A. § 230 (West Supp. 1999).

33. For recent court interpretations of this statute, see *Zeran v. America Online Inc.*, 129 F.3d 327 (4th Cir. 1997), and *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.C.C. 1998).

thousand individuals? As tempting as it may seem, the answer should be "no."

As Professor Eugene Volokh reminds us in his recent article, most regulatory protections of privacy are concurrently restrictions on speech.[34] In order to avoid a potentially unconstitutional chilling of protected speech, I suggest that the FTC use a narrow analysis when determining whether a site is "directed to children." If a site can show that children under 13 (or their parents) do not make up a majority of the visitors, then I think the site should be considered a "general audience site," requiring actual knowledge that they are dealing with a child. To place all sites that have a significant number of participants under age 13 in the "directed to children" category, would, in my opinion, stretch COPPA's reach too far and would chill many web sites and services available to teenagers and young adults.

C. Issues for Implementation

1. What is "actual knowledge"?

Once a web site has determined that it is not directed to children, it need only worry about COPPA to the extent that it has actual knowledge that it is collecting information from a child. But what is "actual knowledge" and, as some clients ask, "How can I avoid it?"

Many general audience web sites collect date of birth information for password verification or just for marketing reasons. With COPPA, any site that collects this information and associates it with personally identifiable information will have "actual knowledge" that they are dealing with a child. For many sites the burden of complying with COPPA's mandate to seek parental consent for those who identify themselves as under age 13 outweighs the benefit of collecting the age data. As a result we will increasingly see notices that registration is not allowed to those under age 13. Other sites may move to merely collecting broad age range data, by for example, asking new registrants if they are "Under 18," "18-35" or "over 35." These ranges may serve the marketing needs without conveying "actual knowledge" upon a company about whether a particular user is under age 13.

The FTC will be on the lookout for web sites who do not ask for age but who ask for information that conveys the same idea. The

34. *See* Eugene Volokh, *Freedom and Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, STAN. L. REV. (forthcoming) (on file with the Santa Clara Computer and High Technology Law Journal).

FTC "will examine closely sites that do not directly ask age or grade, but ask "age identifying" questions such as "what type of school do you go to: (a) elementary; (b) middle; (c) high school; (d) college."[35]

It will be interesting to see how general agency law principles are applied to the COPPA version of "actual knowledge." When will a company be considered to have actual knowledge obtained by its third-party agents? In the comments accompanying the Rule, the FTC discussed the potential liability for affiliates and stressed that the most important factor for determining whether a company will be considered an "operator" is its relationship to the information collected and whether it has an interest in the data.[36] "The [FTC] likely will not pursue an entity that is an 'operator,' but has not facilitated or participated in, and has no reason to know of, any Rule violations."[37] The message seems to be that if a web site values the information it collects from its users, then the site better make sure that both its employees and third party service providers know how to play by COPPA's rules.

An example of a gray area involves the common practice on large interactive web sites of letting certain users become "SYSOPS" to monitor chat rooms. Many of these positions do not rise to the level of employee and yet the SYSOPS have the ability to remove postings or block certain users from the chat and bulletin board areas. Will a SYSOPS be considered an agent of a company such that if the SYSOPS learns of a child disclosing personal information in a chat area, the company itself will be deemed to have actual knowledge? The FTC Statement did not clarify this point but it will likely come up. In the meantime, there is certainly no harm for an on-line service provider to instruct SYSOPS on what to do if they do notice a child disclosing personal information in a public area of the web site.

2. Verifiable Parental Consent

For web sites directed to children and for general audience web sites who learn that they are dealing with a child, the issue of obtaining parental consent prior to collecting personal information becomes a key issue. The Rule states that: "Before collecting, using or disclosing personal information from a child, an operator must

35. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59892 (1999) (to be codified at 16 C.F.R. pt. 312).

36. *See id.* at 59891.

37. *Id.* at 59891 n.55.

obtain verifiable parental consent from the child's parent."[38] The FTC has offered some significant guidance in this area. It has called for "reasonable efforts," taking into consideration "available technology"[39] and refers to the following methods as sufficient to satisfy the requirements:

- Providing a consent form to be printed out and sigend by the parent and returned by postal mail or fax;
- Requiring a parent to use a credit card to demonstrate adult status;
- Having a parent call a toll-free number staffed by personnel trained to determine if the person is an adult;
- Verifiying a parent's digital certificate using public key technology; and
- Email approval accompanied by a PIN or password obtained through one of the above methods.[40]

In addition, until April 21, 2002, companies that will only be using children's personal information for internal purposes may obtain consent using a parent's e-mail address (collected from the child) so long as this is coupled with an additional verification step such as a follow up telephone call, letter or e-mail. This is called the "sliding scale" approach and will be reevaluated by the FTC in light of advances in technology and verification options in the next two years.[41]

Choosing between the various methods will require a thoughtful cost benefit analysis. The implementation and operational requirements for each method vary and for most companies, the decision requires a high-level corporate buy-in. For some companies, the results of the inquiry into what type of consent to require have been startling enough to dissuade them from collecting information from children altogether or from allowing children to use their site. For web sites directed to children, this may be the hoped-for result of the new law. For general audience sites, it may just mean that we will have less data about what children under 13 are doing because they will increasingly identify themselves as older to obtain access to web sites.

38. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (1999).

39. *Id.* § 312.5(b).

40. *See id.*

41. *See id.*; *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59901.

One benefit that some sites are finding as a result of seeking parental consent is the development of a positive relationship with the parents. Parents will generally appreciate being notified about their child's activities on the Internet and may think highly of a company for seeking their involvement.

3. Safe Harbors

There are a few safety-zones in the new law – instances where the collection of personal information from a child are excepted.

The first thing to note in this regard is that COPPA only applies to personal information obtained on-line after April 21, 2000. COPPA does not reach data collection done through other means such as mail-in contests, shopping malls, sports camps etc.[42] Also, personal information collected prior to April 21, 2000 is not covered under COPPA, but additions to this information would be. So, for example, if a web site has many registered users who are under 13, they do not need to cancel these childrens' accounts but the web site may not gather additional personal information from the child without obtaining parental consent. In addition, COPPA provides that the following collections of personal information from a child do not require parental consent:[43]

- Contact information collected for the sole purpose of obtaining parental consent;[44]
- Contact information to be used on a one-time basis to respond to a specific request of a child. For example, a site may use the email address of a child to respond to an email request from the child (note: cannot use the data again and must delete after the one-time use);[45]
- Contact information to be used to respond on a repetitive basis to a single request and not for any other use.[46] For example, a site will not be deemed to have "collected information from a child" if the child merely signs up for an email newsletter and the child's email address is not used for any other purpose. If

42. In the FTC's proposed rule, issued April 27, 1999, the FTC had extended the reach of COPPA to these offline areas, but the Act as passed by Congress applied only to on-line collections of information so the FTC narrowed the scope in the final rule.

43. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(c) (1999).

44. *See id.* § 312.5(c)(1).

45. *See id.* § 312.5(c)(2).

46. *See id.* § 312.5(c)(3).

the site is directed to children or is aware that the recipient is a child, the site must take reasonable steps to provide notice to the parent via letter or via the parent's email address;

- Contact information to be used to protect the safety of a child and to be used solely for that purpose.[47] This exception also required reasonable efforts to provide notice to the parent. It is difficult to predict the situations in which this exception would be applicable;
- Contact information collected to the extent reasonable to (i) protect the security or integrity of the website; (ii) to take precautions against liability; (iii) to respond to judicial process; or (iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.[48]

Finally, the FTC does offer the option for companies, organizations or groups, to apply for and receive approval of a self-regulatory plan regarding collection of on-line information from children.[49] These self-regulatory guidelines are referred to as "Safe Harbors" and at least one company has already applied for one to cover its Privacy Seal program.[50]

III. CONCLUSION

As the FTC begins to bring enforcement actions under COPPA, some of the questions I have raised in this article will surely be answered and some gray areas clarified. Until then, I recommend a careful reading of the Rule for any commercial web site that is directed to, targeted to, or used by children.

Hopefully, the FTC will be able to use COPPA to shut down the truly bad actors who collect information from children for improper purposes. In the process, however, many on-line companies collecting information without any nefarious purpose will be

47. *See id.* § 312.5(c)(4).

48. *See id.* § 312.5(c)(5).

49. *See* 16 C.F.R. § 312.10(a) (1999).

50. PrivacyBot.com became the first organization to submit a letter requesting "safe harbor" classification. *Request for "Safe Harbor" Seal Program Status Under COPPA*, Letter from PrivacyBot.com to Donald S. Clark, Secretary of the FTC (Dec. 15, 1999). See <http://www.ftc.gov/privacy/safeharbor/shp.htm> for links to this request and other FTC announcements related to COPPA's Safe Harbors.

scrutinized as well. The important sound bite for such law-abiding companies to hear is that complying with COPPA, or any new law concerning collection and use of information, may not be simple or painless and therefore deserves thoughtful attention and resources. For many in the Internet industry, COPPA will be just the incentive they need to evaluate their collection and use of consumer information before the rest of the tide of privacy regulations rolls in.

PRIVACY ON THE INTERNET: THE EVOLVING LEGAL LANDSCAPE

Prepared Remarks of

Debra A. Valentine[†]

TABLE OF CONTENTS

I. INTRODUCTION

The Internet has evolved from a communications link among defense researchers into a network providing millions of users easy access to a wealth of information, goods, and services. Currently, it is estimated that well over 100 million people have access to the Internet, and the number is growing quickly.[1] In part, the exponential growth in the on-line consumer market has propelled the Internet's extraordinary growth. As the Federal Trade Commission (FTC or "Commission") noted in its July 1999 report to Congress, on-line commerce tripled from approximately $3 billion in sales in 1997 to

---

† General Counsel of the United States Federal Trade Commission. Ms. Valentine previously served as Assistant Director for International Competition and Deputy Director for Policy Planning at the FTC. Before serving with the FTC, she was a partner at O'Melveny & Myers. Ms. Valentine graduated from Yale Law School and received her undergraduate degree from Princeton University. The views expressed here are those of the author and not necessarily of the Federal Trade Commission or any Commissioner.

1. *See* Cass R. Sunstein, *Code Comfort*, THE NEW REPUBLIC, Jan. 10, 2000, at 37; Nielsen//Netratings, *Weekly Internet Ratings, Data for Monday, January 3 through Sunday, January 9, 2000* (Jan. 13, 2000) <http://www.nielsen-netratings.com/press_releases/pr_000113.htm>.

approximately $9 billion in 1998.[2] Annual consumer sales are projected to skyrocket from $15 billion in 1999 to $184 billion in 2004.[3]

The Net is transforming not just our economy, but also our society and our notions of privacy. While the Internet provides a goldmine of information, products, and services to consumers, the Internet also is a rich source of information *about* consumers. Internet sites collect substantial amounts of personal information, both directly through registration pages, survey forms, order forms, and on-line contests, and indirectly through software products such as "cookies" and other types of tracking software.[4]

By following consumers' on-line activities, Internet site owners and other data collectors gather significant information about visitors' personal interests and preferences. Such consumer data have proven to be extremely valuable to on-line companies—they enable on-line marketers to target products and services tailored specifically to the interests of individual consumers and permit companies to boost their revenues by selling the data or selling advertising space on their Internet sites.[5] An entire industry has emerged to market a variety of software products designed to assist Internet sites in collecting and analyzing visitor data and in serving targeted advertising.[6]

Ultimately, the prevalence, ease, and relatively low cost of collecting, maintaining, and disseminating personal consumer information have a Janus-faced aspect. On the one hand, the ability to gather, process, and disseminate information on the Internet provides

---

2. FTC, SELF-REGULATION AND PRIVACY ONLINE: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS 1 (July 1999) <http://www.ftc.gov/os/1999/9907/privacy99.pdf> [hereinafter FTC'S JULY, 1999 PRIVACY REPORT]; *see also* FTC, THE FTC'S FIRST FIVE YEARS: PROTECTING CONSUMERS ONLINE 3 (Dec. 1999) <http://www.ftc.gov/os/1999/9912/fiveyearreport.pdf>.

3. Actual sales for 1999 are not yet available, but the FTC has projected figures of $12 to $18 billion. *See* FTC'S JULY, 1999 PRIVACY REPORT, *supra* note 2, at 3; *see also* Forrester Research, Inc., *Online Retail to Reach $184 Billion by 2004 as Post-Web Retail Era Unfolds* (Sept. 28, 1999) <http://www.forrester.com/ER/Press/Release/0,1769,164,FF.htm>.

4. *See* John Markoff, *Bitter Debate On Privacy Divides Two Experts* (Dec. 30, 1999) <http://www.nytimes.com/library/tech/99/12/biztech/articles/30privacy.html>. Cookie technology allows a web site server to place information about a consumer's visits to the site on the consumer's computer in a text file readable only to that web site server. The cookie assigns each consumer's computer a unique identifier so that the consumer can be recognized in later visits to the site. Advertisers are now able to assign a cookie to the computers of users who visit sites in advertising networks and to follow those users from site to site by reading information stored in that cookie at each site.

5. *See* FTC'S JULY, 1999 PRIVACY REPORT, *supra* note 2, at 2.

6. *See id.*; *see also supra* note 4.

consumers with a wealth of benefits (*e.g.*, web sites can "remember" where a consumer has been and what type of products the consumer likes so that when the consumer returns to the site, she can be directed to additional products that are likely to interest her). On the other hand, darker voices are legitimately concerned that the manipulative use of information available on the Net may adversely affect privacy.[7] Some uses of personal data can be intrusive, as when private information is widely circulated; or reckless, as when inaccurate information is widely shared with other people and companies; or predatory, as when the information is used to target victims for a scam or crime.

For over five years, the FTC has actively monitored developments in e-commerce, particularly those affecting consumer privacy. The FTC has supported industry self-regulation and has taken enforcement actions as needed. The FTC also has endorsed certain legislative initiatives (*e.g.*, the Children's Online Privacy Protection Act[8]) to address specific on-line privacy concerns. As explained below, there is no simple choice between self-regulation or legislation as the anointed vehicle for protecting consumers' privacy. We already have both and will continue to need both in the future.

II. PRIVACY ON THE INTERNET—THE EVOLVING LEGAL LANDSCAPE

In the United States, individual privacy, including on-line privacy, is protected through a combination of constitutional guarantees, federal and state statutes, regulations, and voluntary codes of conduct, all of which apply to the public and private sectors in different ways. Although the U.S. Constitution does not explicitly mention a right to privacy, the Supreme Court decades ago recognized a fundamental right to privacy, or the right to be left alone.[9] The Court subsequently interpreted the Bill of Rights as creating, through a penumbra of various rights, "a right of personal privacy, or a guarantee [that] certain areas or zones of privacy [do] exist under the Constitution."[10] Viewed in hindsight, the federal courts have effectively acknowledged a right to privacy with respect to marital relations, procreation, contraception, family relationships,

7. *See* Sunstein, *supra* note 1, at 37; *see also* Glenn R. Simpson, *E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise*, WALL ST. J., Jan. 6, 2000, at A24.

8. 15 U.S.C.A. §§ 6501-6506 (West Supp. 1999).

9. *See* Griswold v. Connecticut, 381 U.S. 479, 483-86 (1965).

10. Roe v. Wade, 410 U.S. 113, 152 (1973).

child rearing, and education.[11] In addition, a number of state constitutions specifically enumerate the right of citizens to be protected from privacy invasions.[12]

Aside from constitutional guarantees, the U.S. legislative approach to privacy has been traditionally sectoral, that is, privacy law has developed to address particular data types and users.[13] Historically, fear of the government's use of personal data was the primary concern. Certain statutes thus limit the use of personally identifiable data that the government maintains.[14] Other statutes limit the government's use of personal data maintained by industry.[15] And some statutes limit firms' use of personal data.[16] While no single law or regulation specifically recognizes a U.S. citizen's general right to *informational* privacy, certain laws as applied do afford a fair amount of such privacy to consumers.

A. Federal Trade Commission Act and Informational Privacy

Section 5 of the Federal Trade Commission Act[17] ("FTC Act") in

---

11. *See, e.g.*, Loving v. Virginia, 388 U.S. 1 (1967) (marital relations); Skinner v. Oklahoma, 316 U.S. 535 (1942) (procreation); Eisenstadt v. Baird, 405 U.S. 438 (1972) (contraception); Prince v. Massachusetts, 321 U.S. 156 (1944) (family relationships and child rearing); Pierce v. Society of Sisters, 268 U.S. 510 (1925) (education).

12. *See, e.g.*, CAL. CONST. art. I, § 1; ARIZ. CONST. art. II, § 8; ILL. CONST. art. I, § 6.

13. *See, e.g.*, Driver's Privacy Protection Act of 1994, 18 U.S.C.A. §§ 2721-2725 (West Supp. 1999). The DPPA regulates the disclosure and resale of personal information contained in records that state Departments of Motor Vehicles maintain. Recently, the state of South Carolina challenged the statute's constitutionality, arguing that it violated fundamental principles of federalism. The U.S. Supreme Court upheld the statute. *See* Reno v. Condon, 120 S. Ct. 666 (2000) (2000 U.S. LEXIS 503).

14. For example, the Tax Reform Act of 1976, 26 U.S.C. § 6103 (1994 & Supp. I 1995), protects the confidentiality of tax returns and return-related information and limits the dissemination of individual tax return data. Another example is the Privacy Act of 1974, 5 U.S.C. § 552a (1994), which regulates the government's creation, collection, use, and dissemination of records which can identify an individual by name or other personal information.

15. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522, 2701 (1994), *as amended*, which limits the circumstances under which the federal *and* state governments may access oral, wire, and electronic communications.

16. Privacy statutes that regulate private industry include the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1994) (bank records); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994) (credit reports and credit bureaus); Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1994) (barring video stores from disclosing customers' video choices); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1994) (educational institutions' informational records); Employee Polygraph Protection Act, 29 U.S.C.A. §§ 2001-2009 (West Supp. 1999) (limits employers' ability to use polygraphs); Telemarketing Protections Act, 47 U.S.C. § 227 (1994) (limits on use of automatic dialing machines in telemarketing); and the Cable Communications Policy Act, 47 U.S.C. § 551(a) (1994) (cable television).

17. 15 U.S.C. § 45(a) (1994).

particular can protect consumers' informational privacy whenever a company collects or disseminates personal data in an unfair or deceptive manner. For example, in August 1998, the Commission brought its first on-line privacy case against GeoCities.[18] In that case, the Commission was concerned that GeoCities, one of the most frequently visited sites on the Web,[19] collected personal identifying information from its members, both adults and children, and misled them as to its use of that information. When visitors become members, they must fill out an on-line application that requires disclosure of certain personal identifying information and requests optional information regarding education level, income, marital status, occupation, and interests. Through the registration process, GeoCities created a database rich with target markets for advertisers. The Commission alleged in its complaint that GeoCities falsely represented that the mandatory information that members provided would not be released to third parties without permission. In addition, GeoCities collected personal identifying information from children, for whom it promotes a GeoKidz Club[20] that offers activities, contests, and games. The FTC charged that GeoCities misrepresented that it alone maintained this identifying information from children, when in fact a third party collected and maintained it.

Ultimately, GeoCities settled the case by agreeing to disclose prominently on its web site just what information it collects, for what purpose, to whom it will be disclosed, and how consumers can inspect and, if desired, remove their personal information from the databases of third parties. The consent order also prohibits GeoCities from misrepresenting who is sponsoring the various activities offered on its web site and who actually is collecting and maintaining personal information. Finally, to protect children, the order requires GeoCities to obtain parental consent before collecting information from those age 12 or younger, and to delete any such information already collected, unless GeoCities obtains affirmative parental consent to retain it.[21]

The comprehensive GeoCities consent agreement helped to establish some of the key elements of fair information practices that

18. *See In re* GeoCities, Inc., No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999). Since the time of the settlement, GeoCities has become part of Yahoo!.

19. GeoCities offers its members free and fee-based personal home pages, and links its members' home pages into a virtual community of themed neighborhoods. *See* <http://geocities.yahoo.com>.

20. The GeoKidz Club has been replaced by a kids' club called the Enchanted Forest.

21. *See GeoCities*, 1999 FTC LEXIS 17, at *19-21.

protect consumers' on-line privacy. Those elements include: 1) ***notice*** of the site's privacy practices; 2) consumer ***choice*** regarding the use of information collected; 3) consumer ***access*** to correct or remove personal information; 4) safeguarding the ***security*** of information; 5) ***parental control*** over the collection and use of information gathered from children; and 6) an ***enforcement*** mechanism to ensure compliance.[22] These are precisely the types of protections that the Commission has been urging web site operators to provide voluntarily through self-regulation.[23] ***Enforcement/Redress*** recognizes the principle that an enforcement mechanism is vital to ensure compliance with all the other fair information practices and to provide recourse for injured parties. A self-regulatory program that seeks to assure enforcement and redress might incorporate such

---

22. These core information privacy principles have developed from studies, task forces, directives, and reports, including: U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973); U.S. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977); ORG. FOR ECON. COOPERATION AND DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980); U.S. INFO. INFRASTRUCTURE TASK FORCE, INFO. POLICY COMM., PRIVACY WORKING GROUP, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995); U.S. DEP'T OF COMM., PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995); DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (1995); CANADIAN STANDARDS ASS'N, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION: A NATIONAL STANDARD OF CANADA (1996). *See generally GeoCities*, 1999 FTC LEXIS 17, at *21-8.

23. *See* FTC'S JULY, 1999 PRIVACY REPORT, *supra* note 2, at 3-4. The FTC now recognizes five widely accepted principles essential for effective self-regulatory (or legislative programs) to protect privacy. These five principles are:

Notice/Awareness is the most basic principle. All web sites should disclose to consumers the site's information use and privacy protection policies such as: 1) what information is being collected; 2) who is collecting it; 3) how it will be used; 4) who might have, or will be given access to the data; 5) what passive or non-obvious, data collection methods are used by the site; 6) whether providing the requested information is mandatory or voluntary; and 7) how the data will be protected.

Choice/Consent embodies the principle that web sites should seek consumers' consent regarding any uses of the information beyond those necessary to achieve the basic purpose of the data request.

Access/Participation establishes the principle that consumers should be able to access data about themselves and to challenge the data's accuracy or completeness. Timely and inexpensive access, a means for consumers to verify the information recorded in the site's database, and a method to correct information or add objections to the file, are essential for meaningful access.

Integrity/Security reflects the principle that data collectors should ensure that the information they collect is secure and accurate. For example, the collector should use only reputable sources of data, should cross-check data where possible, and take steps to secure the data against loss or unauthorized access.

features as periodic compliance audits, neutral investigation of consumer complaints, a dispute resolution mechanism, and correction of misinformation or compensation for injured parties. These same principles also served as the foundation for the Children's Online Privacy Protection Act that was enacted in 1998 (*see infra*).[24]

Another recent case illustrating section 5 of the FTC Act's ability to protect informational privacy is the Commission's action against ReverseAuction.com.[25] ReverseAuction is an on-line site that features "Declining Price" auctions (that is, the initial, opening price of an item drops the longer the item remains up for auction) and "Wanted" auctions (that is, buyers who are looking for a particular item or service indicate how much they are willing to pay for the item or service, and sellers then try to outbid each other by offering lower prices). The Commission charged that the firm violated consumers' privacy by harvesting consumers' personal information from a competitor's site and then sending deceptive spam to those consumers, soliciting their business.

In essence, it was alleged that, in promoting its new site, ReverseAuction registered with eBay.com, a competitor auction site. ReverseAuction agreed to be bound by eBay's "User Agreement" and "Privacy Policy," which purported to protect consumers' privacy by prohibiting eBay users from gathering and using personal identifying information (such as names and email addresses) for unauthorized purposes such as spam. Notwithstanding that agreement, ReverseAuction harvested eBay's users' personal identifying information and used the data to send them spam promoting ReverseAuction's own web site. ReverseAuction claimed that the spam recipient's eBay user ID would expire soon, when in fact it was in no danger of expiring. By using this deceptive tactic, ReverseAuction lured eBay users to its web site where they could "re-register." The Commission also alleged that consumers believed that eBay had provided their eBay user IDs and other information to ReverseAuction, or at least had authorized these practices. In reality, eBay had no idea that ReverseAuction was engaging in these activities. At the end of the day, those who "re-registered" their eBay user IDs at ReverseAuction's site were simply registering with and

24. 15 U.S.C.A. §§ 6501-6506 (West Supp. 1999).

25. *See Complaint for Permanent Injunction and Other Equitable Relief,* FTC v. ReverseAuction.com, Inc. (D.D.C. Jan. 2000) (visited Mar. 24, 2000) <http://www.ftc.gov/os/2000/01/reversecmp.htm>; *see also Stipulated Consent Agreement and Final Order,* FTC v. ReverseAuction.com, Inc. (D.D.C. Jan. 2000) (visited Mar. 24, 2000) <http://www.ftc.gov/os/2000/01/reverseconsent.htm>.

becoming a member of ReverseAuction.com with their eBay IDs now also serving as their ReverseAuction IDs.

The proposed settlement bars ReverseAuction from making any misrepresentations about complying with another company's user agreement, privacy policy, or other provisions that govern the collection, use, or disclosure of consumers' personal identifying information. In addition, ReverseAuction is barred from making any misrepresentations about the features, terms, conditions, business practices, or privacy policies of any other company. Furthermore, the proposed settlement requires ReverseAuction to send an e-mail message to all consumers to whom it had sent spam, explaining that ReverseAuction had not intended to suggest that consumers' eBay user IDs would expire and stating that eBay did not know about and had not authorized any of ReverseAuction's actions. The e-mail will inform consumers that their names and eBay user IDs can be purged from ReverseAuction's database and their registration canceled. Finally, the proposed settlement requires ReverseAuction to post its own privacy policy on its Internet web site and maintain certain records to enable the FTC to monitor compliance with the proposed settlement.

This case illustrates both section 5 of the FTC Act's broad authority and the Commission's commitment to protecting consumers' privacy on-line whenever that privacy is threatened. Here, the FTC was able to ensure that the privacy protections assured to eBay's users were not compromised when the deceptive tactics of a competitor auction site thwarted eBay's self-regulatory efforts to protect consumers' privacy. Without actions such as this one, consumers will lose confidence about whether their privacy choices will be honored. And, because consumer confidence is critical to the development of e-commerce in general, cases such as this one are essential for fostering the continuing growth of e-trade.

B. Other Federal Statutes and Informational Privacy

In addition to the FTC Act, a few other federal statutes, such as the Fair Credit Reporting Act (FCRA),[26] Title V of the Gramm-Leach-Bliley Act,[27] and recently proposed regulations from the Department of Health and Human Services, provide a certain amount of informational privacy protection. While earlier statutes, particularly

26. 15 U.S.C. §§ 1681-1681t (1994).

27. Pub. L. No. 106-102, 113 Stat. 1338, 1436-1450 (1999) (to be codified at 15 U.S.C. §§ 6801-6809).

the FCRA, may have been conceived for an off-line world, they function to protect the privacy of both on- and off-line consumers. Indeed, it is becoming increasingly difficult to meaningfully protect privacy without addressing concerns in both the real and virtual worlds. This will become even more true as companies begin to merge on-line and off-line consumer data and profiles.

First enacted in the 1970s, the FCRA regulates consumer reporting agencies, also known as credit bureaus, and establishes important protections for consumers with respect to the privacy of their sensitive financial information that credit bureaus hold. The FCRA allows credit bureaus to disclose consumer credit reports only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment, or other, similar purposes).[28] Moreover, these disclosures can only occur under specified conditions (such as certification of need from a prospective employer or insurer). In these ways, the FCRA generally limits the disclosure of consumer reports primarily to instances where a consumer initiates a transaction, such as a loan or employment application. Of course, these processes can now occur completely on-line.

There are certain caveats associated with the FCRA. First, in contrast to credit bureaus with their rich, accurate and up-to-date data collections, individual merchants, both on- and off-line, are free to distribute any information that they collect as part of their discrete transactions or experiences with consumers.[29] Second, the 1996 amendments to the FCRA include a provision that permits "affiliated" companies to share consumer reports, so long as consumers are notified and given the opportunity to prevent such sharing.[30] Sharing financial information among affiliated companies may well raise special concerns in the electronic banking or electronic payments context, where detailed and sometimes sensitive information about consumers is gathered.

Congress recently enacted financial privacy provisions in Title V of the Gramm-Leach-Bliley Act, which add to the legal protections

28. 15 U.S.C. §§ 1681-1681t.

29. *See Id.* § 1681a(d)(2) ("The term 'consumer report' does not include (A) any report containing information solely as to transactions or experiences between the consumer and the person making the report.").

30. *Id.* § 1681a(d)(2)(A)(iii). Note, moreover, that affiliates may freely share among themselves their individual transaction and experience data without providing any notice or opportunity to object to consumers. *Id.* § 1681a(d)(2)(A)(ii).

available for consumers' financial information.[31] Under Title V, banking institutions may share personal confidential financial information with their affiliates, but not with third parties such as on-line marketers, unless consumers are first notified and given the option to require that the banking institution keep all information private.[32] Even with respect to affiliated entities, Title V requires financial institutions to disclose their privacy policies to their customers, including any intent to share nonpublic personal information.

Finally in the extremely sensitive area of medical records, the Department of Health and Human Services recently issued proposed regulations establishing the first-ever national standards to protect health information that is transmitted or maintained electronically.[33] Among other things, the proposal would require an individual's written consent to release medical information for purposes unrelated to treatment and payment. A notable loophole in the proposed rules is that the rules would not protect health information if it is transmitted or maintained solely via traditional, paper records.

C. Federal Internet-Law

Specific federal protections for consumer privacy on the Internet are fairly limited. Most notably, the Children's Online Privacy Protection Act (COPPA) requires that operators of web sites directed to children under 13 or who knowingly collect personal information from children under 13 must: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) upon request, provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's on-line participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal

31. Pub. L. No. 106-102, 113 Stat. 1338 (1999).

32. *See Id.* at 1437.

33. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (1999) (proposed rule).

information collected.[34]

COPPA directs the Commission to adopt regulations implementing these requirements, and on November 3, 1999, the Commission published its final rule incorporating and explaining COPPA's privacy protections.[35] The rule provides a safe harbor for operators who follow Commission-approved self-regulatory guidelines. Moreover, the Commission retains its authority under section 5 of the FTC Act to investigate and enforce against any child-related information practices that are deceptive or unfair.[36]

COPPA is a classic example of federal legislation aimed at protecting a particular privacy problem—children's information privacy on the Internet. The lack of much additional federal legislation protecting Internet privacy stems from several sources. First, there is no consensus that one general approach solves all privacy problems. Some believe that firms should always seek consumers' consent before sharing their personal data (the opt-in advocates). Others believe that it is more efficient and beneficial for all involved if firms are allowed to share consumers' personal data so long as they notify consumers and enable them to prevent such sharing before it occurs (the opt-out advocates). Alternatively, it may prove most desirable to have opt-in (affirmative consent) rules for certain types of sensitive data sharing (*e.g.*, medical information) and opt-out rules when less sensitive data is being shared or when there is a broad consensus that such sharing is useful for both consumers and firms.

Second, there is a general reluctance to create a plethora of national or state laws for an inherently global technological environment. There is a legitimate concern that an explosion of various sovereigns' laws regulating the Net would only create conflicts of laws rather than resolve issues of privacy invasion. In addition, there has been at least a tentative conclusion that existing

34. 15 U.S.C.A. §§ 6501-6506 (West Supp. 1999).

35. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888 (1999) (to be codified at 16 C.F.R. pt. 312). Notably, COPPA provides that "[a] violation of a regulation prescribed under subsection (a) [the FTC-promulgated rules] shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. § 57(a)(1)(B))." 15 U.S.C.A. § 6502(c) (West Supp. 1999). By treating a COPPA rule violation as if it were a violation of a rule promulgated under section 18(a)(1)(B), the Commission can seek civil penalties immediately.

36. The FTC did precisely this with the Young Investor web site, which allegedly falsely represented that personal information collected from children in a survey would be maintained anonymously. The case eventually settled. *See Young Investor Website Settles FTC Charges* (May 6, 1999) <http://www.ftc.gov/opa/1999/9905/younginvestor.htm>.

laws, such as section 5 of the FTC Act, combined with self-regulation, may be adequate to protect personal informational privacy on the Net. But that tentative consensus may be falling apart, as businesses and consumers recognize the serious harm that hackers, fraud artists and sheer mistakes can wreak with personal financial and identifying information. Moreover, businesses are beginning to worry about the specter of different state law standards as legislators attempt to respond to citizens' concerns about identity theft and privacy invasions.[37]

III. CURRENT FEDERAL POLICY ON INTERNET PRIVACY

The choice of either legislating privacy on the Net or fostering self-regulation is a false one. In fact, we already have both. However, there are legitimate reasons why federal policy regarding privacy on the Internet thus far has favored a self-regulating cyberspace marketplace.

Given the rapidly evolving nature of the Internet and computer technology, self-regulation is the least intrusive and may be the most efficient means to ensure fair information practices.[38] Voluntary codes are by definition developed and adopted by those with the greatest expertise about and sensitivity to industry practices and conditions. And self-regulatory codes can be revised when necessary, more promptly than legislative codes. This allows firms to respond quickly to the rapid evolution of the Internet and computer technology and to employ emerging technologies to protect consumers' privacy. Moreover, when regulation is voluntarily-adopted, compliance tends to be broader, and enforcement more prompt than when a legislature or agency imposes its mandate. And self-regulation wholly avoids many of the First Amendment issues associated with governmental regulation. Finally, where an industry can regulate itself, the government need not devote as many of its limited resources to the task.

Self-regulatory efforts, of course, may fail—they may not be rigorously implemented or enforced, or they may lapse into a vehicle for exclusionary or collusive conduct among rivals. Businesses may be reluctant to disclose to consumers what they do with personal data, simply to avoid having to compete for customers based on how firms protect personal data. Government vigilance is therefore appropriate

37. *See* Simpson, *supra* note 7, at A24.

38. *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS, at Conclusions section (June 1998) <http://www.ftc.gov/reports/privacy3/index.htm>.

and necessary, especially where business rivals, who have an incentive to restrain competition, are involved in the process.

The Commission's numerous activities to monitor industry efforts to protect consumers' privacy include public workshops, Commission Task Forces, creation of an Advisory Group, and surveys of web sites' privacy practices. The Commission's most recent workshop, jointly sponsored by the U.S. Department of Commerce, focused on on-line profiling.[39] This workshop examined the use of "cookies" and other types of tracking software—and even methods of combining this information with personal information collected directly from consumers or contained in other databases—to create targeted, user-profile based advertising campaigns. Some maintain that no personally identifiable information is collected by this profiling—at most the profile is of the browser or the computer hardware without a street, e-mail address or name attached. But consumer groups and privacy advocates have raised concerns about these practices, primarily because many consumers are unaware that software can be used to create on-line profiles about them. Privacy advocates believe that consumers should at least be given notice that such profiling is occurring and given the choice of whether an on-line profile can be created, maintained, and used. I confess to having some sympathy with that position.

The Commission has also used Task Forces to grapple with various Internet privacy issues such as understanding the costs and benefits of implementing fair information practices on-line. The costs and benefits of granting consumer access to their on-line information and guaranteeing the security of personal information have been particularly contentious. Indeed, the benefits and costs are interrelated insofar as increased access to information, at least with today's technology, tends to undermine the security and integrity of the data.

To better address this dilemma, the Commission recently announced the establishment of the Advisory Committee on Online Access and Security ("Advisory Committee").[40] The Advisory Committee is to examine what constitutes reasonable access to personal information, including whether the extent of access provided by web sites should vary, depending upon the sensitivity of the

39. *See* FTC, PUBLIC WORKSHOP ON ONLINE PROFILING (No. 990811219-9219-01) (Sept. 1999) <http://www.ftc.gov/os/1999/9909/FRN990915.htm>.

40. Establishment of the Federal Trade Commission Advisory Committee on Online Access and Security and Request for Nominations, 64 Fed. Reg. 71457 (1999).

personal information collected and/or the purpose for which such information is collected. It will consider whether consumers should be provided access to enhancements to personal information (*e.g.*, inferences about their preferences or purchasing habits). Other issues are whether appropriate and feasible methods exist for verifying the identity of individuals seeking access and whether the difficulty and costs of retrieving consumers' data should be considered. Finally, the Advisory Committee will consider whether a reasonable fee should be assessed for access and whether limits should be placed on the frequency of requests for access.

On the security side, the Advisory Committee will consider how to define appropriate standards for evaluating the measures taken by web sites to protect the security of personal information. That is, it will consider what may constitute reasonable steps to assure the integrity of this information and what measures should be undertaken to protect against its unauthorized use or disclosure. By May 2000, the Advisory Committee will prepare a written report presenting options for implementing these fair information practices along with the costs and benefits of each option.[41]

Finally, the Commission continues to monitor through surveys the progress of firms' privacy efforts and to assess whether self-regulatory programs are in fact fulfilling their promise. The results of past surveys of commercial web sites suggest that on-line businesses are increasingly providing more notice of their information practices. The Commission's 1998 survey found that only 14% of the sites surveyed posted any disclosure regarding their information practices, and even fewer—2%—posted a comprehensive privacy policy. The "most popular" web sites performed better—71% had posted an information disclosure practice or notice.[42] A year later, two other, independent surveys found that 66% of 361 busy web sites surveyed posted at least one disclosure about their information practices, while 93% of the 100 top web sites did.[43] Unfortunately, these same surveys found that very few sites (10% to 22%) posted disclosures

41. The report or excerpts from the report should be available in May 2000 at <http://www.ftc.gov>.

42. *See* FTC'S JULY, 1999 PRIVACY REPORT, *supra* note 2, at 4.

43. *See* Mary Culnan, *The Georgetown Internet Privacy Policy Study: Report to the Federal Trade Commission* (June 1999) <http://www.msb.edu/faculty/culnanm/gippshome.html>; *see also* Online Privacy Alliance, *Privacy and the Top 100 Sites: A Report to the Federal Trade Commission* (June 1999) <http://www.msb.edu/faculty/culnanm/GIPPS/oparpt.PDF>.

covering all the substantive fair information practice principles.[44] Thus, major challenges remain for effective self-regulation.

In March 2000, Commission staff conducted a new Internet survey to assess the progress that commercial web sites have made in implementing all of the fair information practices (notice, choice, access, security, and enforcement),[45] and went beneath the surface to determine whether on-line privacy practices are adequate for enabling consumers to exercise choice about how their personal information is collected and shared.[46] Commission staff analyzed what information a domain collects; whether a privacy policy is posted and what it covers; whether a recognized seal is posted;[47] and whether third party advertisers attempt to place cookies on the site's visitors' computers. The staff hopes to issue its findings in a report by mid-summer.

If self-regulation is to succeed, another critical issue is how to create incentives to encourage the development of privacy-enhancing technologies that will give consumers more control over how and when their personal data is collected and used. One such technology is the World Wide Web Consortium's "Platform for Privacy Preferences" (P3P).[48] The P3P platform would enable web sites to present their privacy policies in such a way that consumers' computers could automatically "read" the policies and automatically "release" information to sites that conform to consumers' pre-programmed choices on acceptable privacy policies. The P3P protocol, however, is still in the drafting stage.

IV. THE U.S. APPROACH TO PRIVACY VERSUS THE E.U. APPROACH

The U.S. approach to protecting consumer privacy on-line—

---

44. *See* FTC'S JULY, 1999 PRIVACY REPORT, *supra* note 2, at 7-8.

45. *See supra* note 22.

46. The survey will cover two data sets: 1) a random sample of 500 domains drawn from a list of the busiest U.S. ".com" sites having an audience of 39,000 unique visitors or more as compiled by Nielsen's Netratings from the month of January 2000; and 2) a review of the busiest 100 domains on the same Nielsen Netratings list.

47. A recognized seal is TRUSTe's seal of fair information practices. *See, e.g.,* Lands' End site at <http://www.landsend.com>; *see also,* Better Business Bureau's seal of approval for approved information practices at BBB*Online* <http://www.bbbonline.org>.

48. The Consortium (W3C) was created to develop common protocols that promote Web evolution and interoperability. It is an international group, jointly run by the MIT Laboratory for Computer Sciences (LCS) in the U.S., the National Institute for Research in Computer Science and Control in France, and Keio University in Japan. Currently, there are more than 260 members in the Consortium. *See W3C Publishes First Public Working Draft of P3P 1.0: Collaborative Efforts by Key Industry Players and Privacy Experts Promote Web Privacy and Commerce* (May 19, 1998) <http://www.w3.org/Press/1998/P3P> (press release).

relying significantly on industry self-regulation with a minimum of legislative and administrative mandates—differs from that of the European Union (E.U.), which relies more on legislative protections. In particular, the E.U. passed a Directive in 1995 that extensively regulates the buying and selling of personal data.[49] The Directive, which took effect on October 25, 1998, specifies common rules that firms must observe when collecting, holding, or transmitting personal data in their business or administrative activities. Most fundamental for firms is an obligation to collect data only for specified, legitimate purposes and to hold only data that are relevant, accurate, and up-to-date. European citizens, in turn, are guaranteed a bundle of rights—a right of access to their personal data; a right to correct any data that are inaccurate; a right to refuse use of their data for activities such as direct marketing; and a right of recourse if unlawful processing occurs.

Significant for the U.S. is that the Directive prohibits the transfer of personal data to any country that does not provide "adequate" (meaning "comparable") protection. Each E.U. member country has been enacting its own laws to implement the Directive. It is still too early to know how stringent the various E.U. member states' laws and policies will be; how strictly they will be enforced; or how flexible their contemplated system of exemptions and special conditions for individual companies will be. Nevertheless, the Directive may impose substantial restrictions on U.S. subsidiaries who buy and sell personal data in the E.U., or on firms that acquire and transmit personal data to the United States.

The U.S. and the E.U. are currently in negotiations to determine how best to harmonize their different approaches to protect personal data. They have been working on developing "safe harbors" that establish a set of criteria which, if met, would allow U.S. companies to do business with European citizens or firms.[50] These "safe harbors" would require U.S. firms to provide: (1) notice of their information practices; (2) choice as to whether and how personal information may be disclosed to third parties; (3) onward transfer of

49. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (visited Mar. 27, 2000) <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html>; *see also* OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (visited Mar. 28, 2000) <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.htm>.

50. *See* U.S. DEPARMENT OF COMMERCE, Draft, INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES (Nov. 15, 1999) <http://www.ita.doc.gov/td/ecom/Principles1199.html>.

personal data to third parties, consistent with the notice and choice provided; (4) security for personal data, whether at its creation, maintenance, use, or transmission; (5) access by individuals to the information that a firm holds about them and the ability to correct, amend, or delete inaccurate information; and (6) enforcement mechanisms to assure compliance with the foregoing principles and recourse for injured persons. Most recently, U.S. and E.U. delegates met in December to try and complete the negotiations on the safe harbors, but the December meeting ended without any definitive conclusions.

V. CONCLUSION

Like the ever-evolving Internet, the legal landscape that applies to the Internet is in motion and will be for years to come. One way to cope with such an ever-changing scene is to allow self-regulation to develop and change along with it. But industry self-regulation may only gradually develop effective enforcement mechanisms and may ultimately provide inadequate protection against highly motivated hackers or fraud artists. Another way is to empower citizens with technology that helps protect their privacy and permits them to assert control over how their personal data are used. But self-help requires considerable consumer education and sophistication and may well fail to protect consumers against surreptitious privacy invasions or identity theft. Finally, legislation may establish protection against specific fraudulent abuses, or for specific groups, such as children, or may even create useful minimum criteria like those established in the Children's Online Privacy Protection Act. But the legislative process can be slow and cumbersome and may lag behind or interfere with technological developments. Thus, neither pure self-regulation, nor consumer education and technological empowerment, nor legislation alone can be the answer. All are needed to ensure meaningful privacy protection on the evolving Net.

CASE NOTES

This section of the Journal is focused on recent cases dealing with developments in intellectual property law, advances in technology, and the Internet. The notes are published in a format that is different from traditional law review articles in that they are brief and focused on a single case or legal issue. Thus, they provide a concise overview of one area of the law. The Journal's goal in publishing these notes in a non-traditional format is to deliver concise, timely, practical, and interesting information on various legal issues that our readers may find useful.

In implementing these notes, we are hoping to generate more interest and feedback regarding the issues that our readers find interesting or pertinent to their practices. In the future, these notes may become a vehicle upon which to facilitate a dialogue between the Journal and the community.

We hope you enjoy them.

WORLD WRESTLING FEDERATION ENTERTAINMENT, INC. v. MICHAEL BOSMAN: A LEGAL BODY SLAM FOR CYBERSQUATTERS ON THE WEB

M. Scott Donahey[†] and Ryan S. Hilbert[††]

I. INTRODUCTION

On January 14, 2000, an arbitration panelist for the World Intellectual Property Organization (WIPO) ordered Michael Bosman of Redlands, California, to transfer ownership of the domain name <worldwrestlingfederation.com> to Stamford, Connecticut-based World Wrestling Federation Entertainment, Inc. ("WWF"), on grounds that Bosman had registered and used the domain name in bad faith.[1] It was the first case ever to be decided under the new Uniform Domain Name Dispute Resolution Policy (the "Policy") adopted by the Internet Corporation for Assigned Names and Numbers (ICANN) on August 26, 1999.[2] From the moment the case was electronically submitted on December 2, 1999, until the time a binding decision was rendered, the entire dispute lasted only six weeks.[3]

[†] Mr. Donahey graduated from the Santa Clara University School of Law, *summa cum laude*, in 1978. He arbitrates, mediates, and litigates intellectual property disputes, and is on two of the three panels accredited by the Internet Corporation for Assigned Names and Numbers to decide cybersquatting disputes.

[††] Mr. Hilbert received his B.A. in History from the University of California, Los Angeles, in 1995, and expects to receive his J.D. from the Santa Clara University School of Law in 2000. Mr. Hilbert would like to thank David Banie for his hard work and dedication in helping to establish the case note program.

1. World Wrestling Federation Entertainment, Inc. v. Michael Bosman, WIPO, No. D99-0001 (Jan. 14, 2000) <http://arbiter.wipo.int/domains/decisions/html/d99-0001.html> [hereinafter *WWF*].

2. *See* Jeri Clausing, *Wrestling Group Wins Back Use of Its Name on Internet*, N.Y. TIMES, Jan. 17, 2000, at C4. As for the process itself, Bosman stated that he felt that it was even-handed: "'I think it's a good organization,' he said [referring to the World Intellectual Property Organization]. 'They were fair and unbiased and it didn't cost me a dime.'" *Id.*

3. See *WWF*, *supra* note 1, for a more detailed description of the Procedural History underlying this case.

II. STATEMENT OF FACTS

The dispute in this case originated in October 1999, when Bosman, a 25-year-old stock broker from Redlands, California, registered the domain name <worldwrestlingfederation.com> with Australian-based Melbourne IT for US$60 and then offered to sell it to the WWF three days later for US$1000.[4] In an e-mail message to the WWF notifying them of his offer, Bosman stated that cybersquatting cases "typically accomplish very little and end up costing the companies thousands of dollars in legal fees, wasted time and energy."[5] Further, Bosman indicated that "[t]he payment of US$1000 would represent more than payment for [his] time and money, but also . . . would serve as consideration for 'the right to current ownership of the domain name "worldwrestlingfederation.com."'"[6]

Rather than agree to Bosman's offer, on December 2, 1999—one day after ICANN's new Domain Name Dispute Resolution Policy had come into effect[7]—the WWF submitted a complaint electronically to WIPO's Arbitration and Mediation Center.[8] In its complaint, the WWF alleged, *inter alia*, that Bosman had registered a domain name that was identical to its registered service mark and trademark and that Bosman had "no rights or legitimate interests in respect to the domain name at issue."[9] The WWF also claimed that Bosman had registered and used the domain name in bad faith.[10]

---

4. *See* Clausing, *supra* note 2; Michael Utley, *Man Loses Match Over Wrestling Site Name*, KNIGHT-RIDDER TRIB. BUS. NEWS, Jan. 15, 2000. Although the address for the World Wrestling Federation's current web site is <www.wwf.com>, Bosman was able to register the domain name <worldwrestlingfederation.com> after ICANN changed its rules, allowing names of up to 63 characters to be registered rather than the traditional 22. *See* Clausing, *supra* note 2.

5. *WWF*, *supra* note 1.

6. *Id.*

7. The first day complaints could be submitted to dispute-resolution providers for disputes involving domain names registered by registrars other than America Online, the NameIT Corp., and Network Solutions under ICANN's new Domain Name Dispute Resolution Policy was December 1, 1999. Complaints concerning domain names registered by the other three providers began to be submitted on January 3, 2000. *See Implementation Schedule for Uniform Domain Name Dispute Resolution Policy*, ICANN (visited Feb. 24, 2000) <http://www.icann.org/udrp/udrp-schedule.htm>.

8. *See WWF*, *supra* note 1.

9. *Id.* In addition to the above, the WWF also alleged that Bosman had "not developed a Web site using the domain name at issue or made any other good faith use of the domain name," and that the domain name was "not, nor could it be contended to be, a nickname of [Bosman] or other member of his family, the name of a household pet, or in any other way identified with or related to a legitimate interest of [Bosman]." *Id.*

10. *See id.*

Pursuant to paragraph 4(a) of the Policy, the WIPO arbitrator assigned to the case considered three elements in rendering a decision.[11] These three elements, all of which the WWF had the burden of proving, were: (1) that the domain name was identical or confusingly similar to its own registered trademark and service mark; (2) that Bosman did not have any rights or legitimate interests in the domain name; and (3) that Bosman had registered and used the domain name in bad faith.[12]

With respect to the first element, the arbitrator concluded that "[i]t is clear beyond cavil that the domain name <worldwrestlingfederation.com> is identical or confusingly similar to the trademark and service mark registered and used by [the WWF]."[13] The arbitrator also determined that Bosman had "no rights or legitimate interests" in the domain name in question.[14] It was the third element, regarding whether Bosman had registered and used the domain name in bad faith, that generated the most discussion.

According to the arbitrator, although it was clear that Bosman had *registered* the mark in bad faith,[15] he must also have *used* the mark in bad faith in order to be held liable.[16] Citing two United States cases[17] and paragraph 4(b)(i) of the Policy[18] as authority, the arbitrator

---

11. *See id.* In particular, paragraph 4(a) of ICANN's Domain Name Dispute Resolution Policy states:

> You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that: (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and (ii) you have no rights or legitimate interests in respect of the domain name; and (iii) your domain name has been registered and is being used in bad faith. In the administrative proceeding, the complainant must prove that each of these three elements are present.

Uniform Domain Name Dispute Resolution Policy, ICANN (visited Feb. 24, 2000) <http://www.icann.org/udrp/udrp-policy-24oct99.htm> [hereinafter *Policy*].

12. *See WWF*, *supra* note 1.

13. *Id.*

14. *Id.*

15. *See id.* (stating that "[s]ince the domain name was registered on October 7, 1999, and since [Bosman] offered to sell it to [the WWF] three days later, the Panel believes that the name was registered in bad faith.").

16. *See id.*

17. The two cases the arbitrator cited were *Panavision International, L.P. v. Toeppen*, 141 F.3d 1316, 1325 (9th Cir. 1998) (holding that defendant's intention to sell the domain name to the plaintiff constituted "use" of the plaintiff's mark), and *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227, 1239 (N.D. Ill. 1996) (noting that defendant's desire to sell the domain name to plaintiff was sufficient to meet the "commercial use" requirement of the Lanham Act). Incidentally, pursuant to paragraph 15(a) of the Rules for Uniform Domain Name Dispute Resolution Policy, "a Panel shall decide a complaint on the basis of statements and documents

determined that the third element could be met if Bosman had attempted to sell or transfer the domain name "'for valuable consideration in excess of' any out-of-pocket costs directly related to [it]."[19] Since Bosman had offered to sell the domain name to the WWF for an amount that was substantially greater than the amount he paid to register it, the arbitrator held that Bosman had used the domain name in bad faith.[20]

As a result of the arbitrator's holding, paragraph 4(i) of the Policy required that "the registration of the domain name <worldwrestlingfederation.com> be transferred to [the WWF]."[21] In addition, pursuant to paragraph 4(k), Bosman had ten days in which to appeal the decision in a court of competent jurisdiction before Melbourne IT was obligated to transfer ownership rights.[22]

---

submitted and in accordance with the Policy, these Rules and *any rules and principles of law that it deems applicable.*" *Rules for Uniform Domain Name Dispute Resolution Policy*, ICANN (visited Feb. 24, 2000) <http://www.icann.org/udrp/udrp-rules-24oct99.htm> (emphasis added). As a result, although it was unnecessary to consider the laws of the United States in rendering a decision, because both of the parties were domiciled in the United States, and United States courts had had recent experience in dealing with similar disputes, the arbitrator looked to these cases for assistance. *See WWF, supra* note 1.

18. Paragraph 4(b)(i) of the Policy states that:

> [C]ircumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name.

Policy, supra note 11.

19. *WWF, supra* note 1.

20. *See id.*

21. *Id.* Paragraph 4(i) of the Policy states: "The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant." *Policy, supra* note 11.

22. *See Policy, supra* note 11. Paragraph 4(k) of the Policy states:

> The mandatory administrative proceeding requirements set forth in paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under paragraph 3(b)(xiii) of the Rules of Procedure. (In general, that

III. ANALYSIS

As the first case decided under ICANN's new Uniform Domain Name Dispute Resolution Policy, the decision regarding ownership of the domain name <worldwrestlingfederation.com> was both closely watched and the subject of much discussion.[23] Originally, ICANN's Policy was a compromise between various constituencies who argued for their particular interests. For example, one group consisted of those that view the Internet as a communications medium where speech should be free and unfettered. This group often distrusts the business community, which it views as having converted a marketplace of ideas into simply a marketplace. Another group was made up of intellectual property owners who view the Internet as a place where unscrupulous individuals can seize their trademarks and service marks and hold them hostage, by registering them as domain names, or by associating those names with scandalous or unseemly content. Even among the intellectual property owners, differences arose between those who had registered marks on the registry of some country, and those who had acquired marks through use, and had not bothered to register. Finally, there was the conflict over the limited number of domains. While a trademark or service mark could be registered by hundreds of different individuals in different markets or with regard to different products and services, there is only one <.com>.

The first case involving the WWF was relatively straightforward. The registrant clearly had no legitimate interest in the domain name at issue and could not demonstrate one. However, imagine if the domain name in question had been not <worldwrestlingfederation.com>, but rather <wwf.com>, and that the

---

> jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See paragraphs 1 and 3(b)(xiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

Id. As a final note, it should also be pointed out that although the WWF could have litigated this case under the United States Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, 113 Stat. 1501, 1537 (1999) (to be codified at 15 U.S.C. § 1125(d)), it elected not to do so in order to "protect [its] intellectual property interests while preserving the relationship between [it] and its fans at a minimal cost to all concerned." *WWF, supra* note 1.

23. More specifically, this case was given substantial attention both in the general press and particularly in Internet-related publications.

registrant's name had been not Michael Bosman, but William Wright Franklin. The analysis of all of the factors would have to have been much more protracted and painstaking in order to reach a just resolution.

Compare the ICANN Policy to the Anticybersquatting Consumer Protection Act (the "Act")[24] recently passed by Congress. Under the Act, *in rem* jurisdiction can be had at the site of the registrar, where the registrar is located in the United States. This means that parties can be forced to travel great distances to attend hearings and the trial of the matter. Since the registrants are often individuals, who may have a legitimate claim to the domain name at issue, the registrants may be spent into submission. The plaintiff may also collect damages against the registrant under the Act, a remedy which is unavailable under the Policy. If what the plaintiff really wants is the domain name registration, damages amount to a form of vengeance.

Under the Policy, the complainant pays a registration fee in an amount dependant upon the provider and the number of panelists (1 or 3) desired. In no event is this fee more than $5,000, and for one panelist, it does not exceed $1,000.[25] Unless the respondent desires a three-person panel when the complainant has elected a single panelist, the respondent pays nothing.[26] A decision is made on the basis of written documents submitted electronically and by courier, and there is no hearing absent a finding of exceptional circumstances.[27] Decisions issue within a short period of time, usually less than thirty days from the constitution of the panel.[28] Decisions are enforced within ten days of their publication on the ICANN web site, unless a party chooses to appeal by filing an action in a court of competent jurisdiction.[29]

Thus the only costs involved in addition to legal representation are any costs for legal representation. These are limited in nature, since there is generally only one written submission per party and no hearings.

---

24 Pub. L. No. 106-113, 113 Stat. 1501, 1537 (1999) (to be codified at 15 U.S.C. § 1125(d)).

25. *See Schedule of Fees (Annex D)*, World Intellectual Property Organization Arbitration and Mediation Center (visited Mar. 13, 2000) <http://arbiter.wipo.int/domains/fees/index.html>.

26. *See WIPO Guide to Domain Name Dispute Resolution*, World Intellectual Property Organization Arbitration and Mediation Center (visited Mar. 13, 2000) <http://arbiter.wipo.int/domains/guide/index.html>.

27. *See id.*

28. *See id.*

29. *See Policy, supra* note 11.

IV. CONCLUSION

The ICANN procedure is designed to be expedient and inexpensive. It provides a level playing field for the parties, and even the unsuccessful party of the first case involving the domain name <worldwrestlingfederation.com> has called it "fair and unbiased."[30] An individual registrant cannot be forced to abandon his claim to the domain name at issue simply because the defense of the matter is more than the individual can pay. It is a process in which the rights and interests of all the constituencies can be considered and balanced. It is not only international in nature, but *anational.* As such, there is no risk that countries will retaliate against national legislation passed in another country which is considered to be unfair or burdensome. It is private justice, sponsored by a private corporation, concerning a medium that developed without the assistance of national legislation or regulation. It should be allowed to develop and respond to the needs of its constituents.

30. Clausing, *supra* note 2.

MULTIVIDEO LAB v. INTEL CORPORATION

Karen A. Gibbs[†]

I. BACKGROUND

Multivideo Labs, Inc. ("MVL") asserted the following causes of action against Intel Corporation ("Intel")[1]: (1) actual and attempted monopolization in violation of Section 2 of the Sherman Act; (2) false advertising in violation of Section 43(a) of the Lanham Act; and (3) tortious interference with prospective business advantage.[2] Intel moved for summary judgment on MVL's claims.[3]

Central to the dispute was Intel's involvement in the Ease-of-Use Initiative ("the Initiative"), which Intel and other computer industry participants hope will increase consumer demand for personal computers ("PCs") by making PCs easier for consumers to use. One of the biggest challenges that the Initiative has taken on is the lack of a standard for peripheral connections to PCs. Because there was no standardized connection, if a consumer wanted to connect a new peripheral to his or her PC, he or she often would have to go through several steps to connect the peripheral, including shutting down the PC, opening up the PC, and adding an insert or a card that would enable the peripheral to connect and work.

To alleviate the peripheral connection problem, the Initiative seeks to establish the reality of "Plug and Play," meaning that a

---

[†] Karen A. Gibbs recently joined Latham & Watkins' Orange County, California office. Prior to joining Latham & Watkins, Ms. Gibbs was an associate attorney at Day Casebeer Madrid & Batchelder LLP in Cupertino, California, and an associate in the technology litigation department of Cooley Godward LLP in Palo Alto, California. Her practice focuses on patent, trademark, copyright, unfair competition, antitrust, and complex technology license disputes in the computer and biopharmaceutical industries. Her represented clients include Sun Microsystems, Inc. and Amgen Inc. In 1991 Ms. Gibbs received a B.A. magna cum laude with distinction, Phi Beta Kappa from the University of California at Santa Barbara. In 1995 she received a J.D. from the University of California Hastings College of the Law where she served as editor in chief of the *Hastings Communications and Entertainment Law Journal* and as a member of the Moot Court Board. The author would like to thank Jennifer Ishimoto for her assistance during the preparation of this Note.

1. Multivideo Labs, Inc. v. Intel Corp., 2000 WL 12122 (S.D.N.Y. Jan. 7, 2000).
2. *See id.* at *12.
3. *See id.* at *1.

customer can simply buy a peripheral device, plug it in, and go to work. To this end, Intel, Compaq, Digital Equipment, NEC, Microsoft, IBM, and Northern Telecom developed a standard and corresponding Universal Serial Bus[4] ("USB") specification ("the Specification") to enable easy attachment of peripherals. The USB technology not only provides a standard for ports and protocols but also provides the means to manage power consumption for a system of computer components. To manage power consumption, the Specification provides a way for the host computer to identify attached peripherals and then, based on a specified power budget for each USB peripheral, to manage power running through the bus in a way that supports as many peripherals as possible. To avoid a system crash, each USB peripheral must be designed and manufactured in conformance with its specified power budget. If a device exceeds its power budget, the manufacturer is required to reengineer the device to fit within its power budget.

To further assist its Plug and Play efforts, the Initiative also promotes the use of USB-compliant extension cables. USB-compliant cables have an upstream USB "A" plug at one end and a downstream USB "B" plug at the other. Series "A" plugs are always oriented upstream, that is towards the PC, and can connect only with "A" sockets, and series "B" plugs are always oriented downstream and can connect only with "B" sockets. Because of this configuration, compliant cables cannot be connected together, or "cascaded." Non-compliant cables use an "A" socket at one end and an "A" plug at the other. Non-compliant cables therefore can be linked together without limit and result in cable lengths exceeding the Specification's five-meter limit–often resulting in a system crash.

Even though Intel's competitive role in the USB market is minimal and intentionally diminishing, Intel has contributed substantial resources to the development and promotion of the USB standard and Plug and Play effort, including creating a group within Intel whose sole responsibility is to support USB. And Intel and the other drafters of the Specification formed the Universal Serial Bus Implementation Forum ("USB-IF"), an unincorporated, voluntary membership organization engaged in all aspects of PC development. USB-IF has over 500 member companies, including MVL. Intel is the designated administrator and Chair of the UBS-IF, and regularly

4. The "bus" refers to the lines through which computer components, including the host computer and computer peripherals, communicate. *See id.* at *2.

answers questions about the interpretation of the Specification without consulting other members.

To further the adoption of the USB Specification, several times each year, the USB-IF sponsors "Plugfests," where the USB-IF tests products for compliance with the USB Specification. If a product passes the test, the USB-IF includes it on an "Integrators' List," which is given to developers and members of the USB-IF. Products on the list are allowed to display USB logos.

So why did MVL sue Intel? MVL's main USB product is the Active Extension Cable ("AEC"), which MVL invented to help PC users connect USB peripherals to PCs or to each other from a distance up to eighty feet. To keep power levels sufficiently high in order to avoid a crash, the AEC used a "repeater" to amplify and sustain electrical signals. Upon completion of the AEC, MVL announced that the AEC was 100% compatible with the Specification and brought it to the April 1998 Plugfest for testing. After testing, however, the USB-IF found that the AEC was not 100% compatible. One of the main problems was that MVL designed the AEC so that a customer could link several AECs together to create a longer cord. With each AEC extension, the level of effectiveness fell. If a customer linked five AECs together, for example, the level of effectiveness fell to 66%.

Despite the AEC's failure to obtain a place on the "Integrators' List," MVL proceeded to manufacture the AEC. And when MVL first launched its AEC product in January 1999, the AEC's packaging prominently displayed the letters "USB." The front of the package even stated that the AEC was "100% Compatible w/ the USB Electrical & Timing Specs for USB hub . . . Connect up to 5 cables in a series."[5] Even the plug itself contained a USB icon.

In response, an Intel employee sent a letter to MVL and other companies believed to be manufacturing AECs stating that the AEC is not USB compliant. The letter also stated that the AEC had no Specification-required hub, which allows a computer to recognize the device when plugged in. The letter asked that MVL cease representing that the AEC was USB compliant unless it was a hub by itself and had passed USB-IF testing. As a result of receiving this letter, one AEC manufacturer ceased negotiating a deal for the purchase of chips that would have enabled the manufacturer to produce AECs, and orders from several customers were "relegated to

5. *Id.* at *11.

the back burner."[6] In other words, there was a "general cooling of the market" for the AEC.[7]

II. HOLDING, RATIONALE AND DISCUSSION

A. *Sherman Act Claims*

MVL alleged both actual and attempted monopolization, but focused on monopoly leveraging—in other words, that Intel used its "monopoly power in one market to gain a competitive advantage in another, albeit without an attempt to monopolize the second market."[8] The court found no genuine issue of material fact for trial because MVL failed to provide evidence that Intel's products compete with the AEC in the relevant market, that Intel's statements were anything but truthful, and that Intel's motives or actions were anti-competitive.[9]

The threshold requirement for establishing a Section 2 claim is whether the defendant has sufficient market power in the relevant market. In antitrust law, the relevant market is the "area of effective competition."[10] Here, MVL defined the relevant market as that for USB interconnect devices. The court, however, found that there was no evidence establishing that MVL and Intel were competitors in the USB interconnect devices market, or that Intel had the requisite market power in the USB market.[11] In fact, the court found that Intel offered credible evidence to the contrary, establishing that Intel offers very few USB products or components, and that it does not manufacture any USB hubs, cables, or other interconnect products.[12] MVL's argument that Intel's Ethernet products "may" be an alternative to USB products and therefore may compete with MVL's products also fell flat.

MVL also tried to argue that Intel leveraged its monopoly in the

---

6. *Id.* at *12.

7. *Multivideo*, 2000 WL 12122 at *12.

8. Section 2 of the Sherman Act provides that "[e]very person who shall monopolize, or attempt to monopolize, or combine or conspire with any person or persons, to monopolize any part of the trade or commerce among the several States . . . shall be deemed guilty of a felony." 15 U.S.C. § 2 (1994). Plaintiffs can bring a variety of claims under Section 2, including claims of illegal monopoly maintenance, monopolization, attempt to monopolize, and in some forums, monopoly leveraging.

9. *See Multivideo*, 2000 WL 12122 at *15.

10. AD/SAT, Inc. v. Associated Press, 181 F.3d 216, 227 (2d Cir. 1999).

11. *See Multivideo*, 2000 WL 12122 at *13.

12. *See id.*

worldwide market for microprocessors.[13] MVL stated that Intel had substantial market power in the market for central processing units ("CPUs") and that Intel exercised that power through the USB-IF to prevent MVL from competing in the market for the USB interconnect products. But the court rejected this argument, too, because MVL's AEC does not compete with products in the microprocessor market. The court cited the Second Circuit's ruling in *Berkey Photo, Inc. v. Eastman Kodak Co.*,[14] which held that a commercial actor can violate Section 2 of the Sherman Act "by using its monopoly power to gain a competitive advantage in another market, albeit without any attempt to monopolize the second market."[15] The court then, referring to *Spectrum Sports, Inc. v. McQuillan*,[16] noted that the idea of monopoly leveraging claims under Section 2 has been questioned by the Supreme Court. The court noted that even if leveraging survived *Spectrum Sports*, the doctrine most likely would be limited to activity that injures competition, not competitors.[17] The court then found no evidence that Intel had used its power in the microprocessor market to exclude competition in the AEC market.[18] Instead, just the opposite, the court found that Intel was enthusiastic to hear about a possible USB-compliant cable and that it encouraged MVL to develop a compliant product.[19]

MVL also contended that Intel employees' statements that the AEC was non-compliant were anti-competitive.[20] To establish that a defendant has engaged in false and misleading advertising, a plaintiff "[m]ust overcome a presumption that the effect on competition of such a practice was de minimis."[21] To overcome the de minimus presumption, a plaintiff must show that the representations were: (1) clearly false; (2) clearly material; (3) clearly likely to induce reasonable reliance; (4) made to buyers without knowledge of the subject matter; (5) continued for prolonged periods; and (6) not

13. *See id.*
14. 603 F.2d 263 (2d Cir. 1979).
15 *Id.* at 275.
16. 506 U.S. 447 (1993).
17. *See Multivideo*, 2000 WL 12122 at *14.
18. *See id.*
19. *See id.*
20. *See id.* at *15.
21. National Ass'n of Pharm. Mfrs., Inc. v. Ayerst Labs., 850 F.2d 904, 916 (2d Cir. 1988).

readily susceptible of neutralization or other offset by rivals.[22] Because MVL admitted that Intel's statements were true, MVL failed to clear even the first hurdle of this standard.[23]

B. Lanham Act Claim

MVL contended that Intel violated Section 43(a) of the Lanham Act by sending a letter to MVL manufacturers and distributors.[24] To establish a Section 43(a) violation, a plaintiff must prove: (1) the statements were false or misleading; and (2) the statements were made in commercial advertising or promotion.[25] The court found that MVL failed to satisfy these two elements of a Lanham Act claim, and granted Intel's motion for summary judgment.

The court found that MVL did not satisfy the requirement that the statements be false or misleading. The court found that the plaintiff "must demonstrate, by extrinsic evidence, that the challenged [statements] tend to mislead or confuse consumers."[26] MVL did not contend that the Intel letter was intentionally deceptive, but only that it was confusing and misleading. MVL claimed that recipients of the letter believed that the AEC did not work. The court, however, found that since there was no evidence that the consumers held this belief, it was not actionable.[27] Additionally, the court found that the AEC failed to meet the Specification's requirements because it lacked the controller to communicate with the computer and connecting five AECs in series as stated on the box resulted in failure.[28]

The court also found that the statements at issue were not in commercial advertising or promotion. "In order for representations to constitute 'commercial advertising or promotion' under [the Lanham Act], they must be: (1) commercial speech; (2) by a defendant who is in commercial competition with plaintiff; (3) for the purpose of influencing consumers to buy defendant's goods or services.... [and;] (4)... disseminated sufficiently to the relevant purchasing public to constitute 'advertising' or 'promotion' within that

22. *See id.* at 916 (internal quotation omitted).

23. *See Multivideo*, 2000 WL 12122 at *15.

24. *See* 15 U.S.C. § 1125(a) (1994).

25. *See id.*

26. Johnson & Johnson * Merck Consumer Pharm. Co. v. Smithkline Beecham, 960 F.2d 294, 297 (2d Cir. 1992).

27. *See Multivideo*, 2000 WL 12122 at *17.

28. *See id.*

industry."[29] MVL provided no evidence to show that the purpose of the letter was to influence the purchase of Intel products. In fact, both parties presented evidence that the motive behind the statements was to promote compliance with an industry standard, which Intel and its employees believed would benefit customers and competition within the personal computing industry.[30]

C. *Tortious Interference with Prospective Economic Advantage Claim*

MVL also alleged that Intel's statements to AEC manufacturers and distributors constituted tortious interference with MVL's business relations.[31] To establish a tortious interference claim, a plaintiff must prove: (1) a business relationship between the plaintiff and a third party; (2) the defendant, knowing of that relationship, intentionally interfered with it; (3) the defendant acted with the sole purpose of harming the plaintiff, or used dishonest, unfair, or improper means; and (4) the relationship was injured.[32]

The court granted Intel's summary judgment motion and dismissed MVL's tortious interference claims. The court found that MVL had offered no evidence to support the third element of its claim by failing to establish, or even contend, that Intel had used "dishonest, unfair or improper means."[33] The court also found that MVL failed to establish that Intel had acted with the sole purpose of harming MVL.[34]

29. Gordon & Breach Science Publishers v. American Inst. Of Physics, 859 F. Supp. 1521, 1535-36 (S.D.N.Y. 1994).

30. *See Multivideo,* 2000 WL 12122 at *17.

31. *See id.* at *18.

32. *See id.* (citing Goldhirsh Group Inc. v. Alpert, 107 F.3d 105, 108-09 (2d Cir. 1997)).

33. *Id.*

34. *See id.*

INTERGRAPH CORPORATION V. INTEL CORPORATION

Richard J. Gray[†] and David Banie[††]

I. BACKGROUND

The parties involved in this case are Intel Corporation ("Intel") and Intergraph Corporation ("Intergraph").[1] Intel, a manufacturer of semiconductors, appealed the grant of a preliminary injunction granted to Intergraph by the United States District Court for the Northern District of Alabama. Intergraph is an original equipment manufacturer, or OEM, which develops, makes and sells computer workstations. From 1987 to 1993 Intergraph's workstations used a microprocessor based on "Clipper" technology. In 1993 Intergraph discontinued use of the Clipper microprocessor and switched to Intel's microprocessor. By 1994 Intel designated Intergraph as a "strategic customer" and provided Intergraph with proprietary information and early access to samples of new microprocessors under non-disclosure agreements. Intergraph retained ownership of patents relating to the Clipper technology.

In 1996 Intergraph asserted claims of infringement of the Clipper patent against several Intel OEM customers. These customers sought indemnification from Intel, and negotiations ensued between Intel and Intergraph in this matter. Although Intel sought a license to the

---

[†] Richard J. Gray is the founder of Outside General Counsel Silicon Valley ("OGCSV") in Menlo Park, California. OGCSV advises Internet and other high technology companies on intellectual property, strategic partnering and other issues. Mr. Gray received a B.A. summa cum laude, Phi Beta Kappa from Boston College and a J.D. from Stanford University where he earned the Kirkwood Awards for Best Oral Advocate and Best Brief. Mr. Gray was the Chair to the Santa Clara County Bar Association High Technology Law Section for 1998 and 1999. Mr. Gray's website can be found at <www.SVlawfirm.com>.

[††] Mr. Banie received his B.S. in Management Science from the University of California, San Diego, in 1996, and expects to receive his J.D. from the Santa Clara University School of Law in 2000. Mr. Banie would like to thank professors J. Thomas McCarthy and Donald S. Chisum for their help in conceiving the case note. Mr. Banie would also like to thank Jennifer Ishimoto, Candice Lee, Janice Chan, Irene Pleasure, Traci Pickering, and Ryan Hilbert for their invaluable assistance.

[1] Intergraph Corp. v. Intel Corp., 195 F.3d 1346 (Fed. Cir. 1999).

Clipper patent, Intergraph rejected the proposed terms as inadequate. As negotiations failed between Intel and Intergraph, Intel discontinued providing technical assistance and other special benefits to Intergraph.

Tensions between the two parties escalated and in 1997 Intergraph filed suit against Intel claiming: Infringement of the Clipper patents, fraud, misappropriation of trade secrets, negligence, wantonness and willfulness, breach of contract, intentional interference with business relations, breach of express and implied warranties, and violation of the Alabama Trade Secrets Act. Thereafter, Intergraph amended its complaint to charge Intel with violations of antitrust laws.

After a hearing for a preliminary injunction, the district court held that Intergraph was likely to prevail on its claims that Intel was a monopolist and had violated sections 1 and 2 of the Sherman Act. As a result, the district court issued a preliminary injunction against Intel which included the following provisions: (1) "Intel shall supply Intergraph with all Intel product information, including . . . technical, design, development, defect, specification, support, supply, future product, . . . ;"[2] (2) "Intel shall supply Intergraph with an allocation, and set aside a supply of microprocessors, semiconductors, chips, and buses ("Chips") on an advance basis for product development . . . ;"[3] (3) "Intel shall supply Intergraph with an allocation, and set aside a supply, of Chips which have been manufactured by or on behalf of Intel for distribution ("Production Chips"), as well as all future chips proposed by, or available from Intel . . . ;"[4] and (4) "Intel shall supply Intergraph with Production Chips not yet available from Intel's authorized distributors . . . . "[5] The district court also found that Intel had a contractual agreement to provide the benefits, including Intel's "continued [product] support," contained in the injunction.[6] Intel appealed this decision to the Federal Circuit Court of Appeals.

II. HOLDING, RATIONALE AND DISCUSSION

On appeal, the Federal Circuit held that the antitrust rulings of the district court were incorrect in law or were devoid of sufficient factual support to present a substantial likelihood of establishing an

2. Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255, 1291 (N.D. Ala. 1998).
3. *Id.* at 1292.
4. *Id.*
5. *Id.*
6. *See id.* at 1282.

antitrust law violation with respect to the issues presented.[7] Specifically, Intergraph did not show a substantial likelihood of success on the merits that Intel violated the antitrust laws in its actions with respect to Intergraph, or that Intel agreed by contract to provide the benefits contained in the injunction.[8] In its own words, the Federal Circuit held that "Intel's conduct with respect to Intergraph [did] not constitute the offense of monopolization or the threat thereof in any market relevant to competition with Intergraph."[9] In so holding, the Federal Circuit rejected the district court's findings that Intel competed against Intergraph in two key markets: (1) the market for high end microprocessors, and (2) the submarket of Intel microprocessors.[10]

The Federal Circuit also rejected Intergraph's argument "that it compete[d] in the microprocessor market by virtue of its Clipper patents."[11] According to the court:

> [T]he patent grant is a legal right to exclude, not a commercial product in a competitive market. Intergraph abandoned the production of Clipper microprocessors in 1993, and state[d] no intention to return to it. Firms do not compete in the same market unless, because of the reasonable interchangeability of their products, they have the actual or potential ability to take significant business away from each other.[12]

Relying on this key holding, the Federal Circuit then discussed, *inter alia*, the following theories relied on by the district court in finding a probable violation of the Sherman Act: (1) the "Essential Facility" doctrine; (2) refusal to deal; (3) leveraging; (4) coercive reciprocity and tying; (5) the use of intellectual property to restrain trade; and (6) breach of contract.[13]

A. The "Essential Facility" Doctrine

First, the Federal Circuit held that the district court erred in

---

7. *See* Intergraph Corp. v. Intel Corp., 195 F.3d 1346, 1352 (Fed. Cir. 1999).

8. *See id.*

9. *Id.* at 1356.

10. *See id.* at 1355.

11. *Id.*

12. *See Intergraph*, 195 F.3d at 1355 (citing U.S. Anchor Mfg., Inc. v. Rule Indus., Inc., 7 F.3d 986, 995 (11th Cir. 1993)).

13. *See id.* at 1367. The Federal Circuit also rejected the district court's finding that Intel was contractually obligated to provide Intergraph with the benefits contained in the injunction, because it found no such contractual promise. *See id.* at 1367.

holding that Intel's actions in withdrawing advance design and technical information violated the Sherman Act under the "essential facility" theory.[14] The essential facility doctrine imposes liability when one firm denies a second firm reasonable access to a product or service that the second firm must obtain in order to effectively compete with the first.[15] In *MCI Communications Corp. v. American Telephone & Telegraph Co.*, the court enumerated the elements of liability under the "essential facilities" theory as "(1) control of the essential facility by a monopolist; (2) a competitor's inability practically or reasonably to duplicate the essential facility; (3) the denial of the use of the facility to a competitor; and (4) the feasibility of providing the facility."[16] Furthermore, "the courts have required anticompetitive action by a monopolist that is intended to 'eliminate competition in the downstream market.'"[17]

The district court found that "the [a]dvance [c]hips [s]amples and advance design and technical information are essential products and information necessary for Intergraph to compete in its markets."[18] According to the district court, Intel's actions in withholding these benefits violated the Sherman Act because "[t]he antitrust laws impose on firms controlling an essential facility the obligation to make the facility available on non-discriminatory terms."[19] Contrary to this finding, the Federal Circuit found that "[a] non-competitor's asserted need for a manufacturer's business information does not convert the withholding of that information into an antitrust violation."[20] The Federal Circuit further noted that "precedent is quite clear that the essential facility theory does not depart from the need for a competitive relationship in order to incur Sherman Act liability and remedy."[21] Specifically, "there must be a market in which plaintiff and defendant compete, such that a monopolist extends its monopoly to the downstream market by refusing access to the facility it controls."[22] As no such competitive relationship is present here, the

14. *See id.* at 1356-57.

15. *See id.* at 1356 (citing Alaska Airlines, Inc. v. United Airlines, Inc., 948 F.2d 536, 542 (9th Cir. 1991)).

16. *See id.* at 1357 (citing MCI Communications Corp. v. AT&T Corp.., 708 F.2d 1081, 1132-33 (7th Cir. 1983)).

17. *See id.* at 1357 (Fed. Cir. 1999) (quoting *Alaska Airlines*, 948 F.2d at 544-45).

18. Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d at 1270.

19. *Id.* at 1277.

20. *Intergraph*, 195 F.3d at 1357.

21. *Id.* at 1356. *See also* Caribbean Broad. Sys., Ltd. v. Cable & Wireless PLC, 148 F.3d 1080, 1088 (D.C. Cir. 1998).

22. *Intergraph*, 195 F.3d at 1357.

essential facility theory did not support the district court's finding of a Sherman Act violation.[23]

B. Refusal to Deal

Second, the district court erroneously found Intergraph likely to prevail on a claim of Intel's violation of antitrust laws based on a theory of refusal to deal.[24] One of the oldest principles of antitrust law is the right to deal, or not to deal, with whomever one pleases. The U.S. Supreme Court has held, "[i]n the absence of any purpose to create or maintain a monopoly, the [Sherman Act] does not restrict the long recognized right of trader or a manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal."[25] However, a "refusal to deal" may raise antitrust concerns when the purpose is to create, maintain, or enlarge a monopoly.[26] Moreover,

> [A] monopolist's unilateral refusal to deal with its competitor (as long as the refusal *harms the competitive process*) may constitute *prima facie* evidence of exclusionary conduct in the context of a section 2 claim. A monopolist may nevertheless rebut such evidence by establishing a valid business justification for its conduct.[27]

In this case, "[a]lthough the district court found that there was a lack of business justification for Intel's actions, there was no showing of harm to competition with Intel; thus the need did not arise to establish the defense of business justification."[28] Furthermore, a manufacturer is "'under no duty to help [plaintiff] or other peripheral equipment manufacturers survive or expand.'"[29] The Federal Circuit further noted the following:

> Although [this court] observed a few rulings wherein a court has, for example, barred the termination of a distributor during litigation, no case has held that the divulgation of proprietary information and the provision of special or privileged treatment to

23. *See id.* at 1358.

24. *See id.* at 1359.

25. *Id.* at 1358 (citing United States v. Colgate & Co., 250 U.S. 300, 307 (1919)).

26. *See id.* at 1358.

27. Data Gen. Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147, 1183 (1st Cir. 1994) (emphasis added) (citing Eastman Kodak Co. v. Image Technical Servs., Inc., 504 U.S. 451, 483 n.32 (1992)).

28. *Intergraph*, 195 F.3d at 1359.

29. *Id.* (quoting California Computer Prod., Inc. v. IBM Corp., 613 F.2d 727, 744 (9th Cir. 1979)).

> a legal adversary can be compelled on a "refusal to deal" antitrust premise.[30]

Likewise, Intel was under no such duty to provide Intergraph with "strategic customer" benefits; absent a showing of harm to competition, Intel's decision to discontinue its prior dealings with Intergraph raised no antitrust concerns.[31]

C. Leveraging

Third, the district court erred in holding that Intel's expansion into the computer workstation and graphic subsystems markets (by virtue of Intel's agreement to purchase Chips & Technology Company, an experienced producer of graphics chips and chip sets) constituted a sufficient foundation, by itself, for a finding of illegal leveraging.[32] In deciding the issue, the court stressed the following:

> Intergraph made no proffer to show that Intel possessed market power in either the graphics subsystems market or the workstation market.... An integrated business does not offend the Sherman Act by drawing on its competitive advantages of efficiency, experience, or reduced transaction costs, in entering new fields. These advantages are not uses of monopoly power.[33]

The district court relied on *Berkey Photo, Inc. v. Eastman Kodak Co.* for the proposition that "the Sherman Act is violated if monopoly power in one market provides a 'competitive advantage' in another market, whether or not there is an intent to create a monopoly in the second market."[34] However, the district court failed to consider that "there was no economic evidence or proffer concerning Intel's participation in the downstream market."[35] To establish illegal leveraging of monopoly power the challenged conduct must "threaten[ ] the [second] market with the higher prices or reduced output or quality associated with the kind of monopoly that is ordinarily accompanied by a large market share."[36]

The Federal Circuit observed that "antitrust liability based on

---

30. *Id.* at 1358.

31. *See id.* at 1359.

32. *See id.* at 1360.

33. *Id. See also* AD/SAT, A Division of Skylight, Inc. v. Associated Press, 181 F.3d 216, 230 (2d Cir. 1999).

34. *Intergraph*, 195 F.3d at 1359 (citing Berkey Photo, Inc. v. Eastman Kodak Co., 603 F.2d 263, 275 (2d Cir 1979)).

35. *Id.* at 1359.

36. *Id.* (citing 3 PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW § 652C, at 90 (rev. ed. 1996)).

leveraging of monopoly power is a concept of imprecise definition, for the courts have varied in their requirements of the nature of the advantage obtained in the assertedly leveraged market."[37] Furthermore, the court noted that the Second Circuit has rejected the type of broad reading of *Berkey Photo* that the district court has adopted.[38] Specifically, the Second Circuit held that a "Sherman Act violation based on leveraging requires a showing of 'tangible harm to competition' in the second market."[39]

The Federal Circuit further noted that other circuits have explicitly rejected *Berkey Photo*.[40] For example, the Third Circuit held that "a section 2 leverage claim requires the use of monopoly power in the second market, and that a mere attempt to gain a competitive advantage is insufficient as a matter of law."[41] The Ninth Circuit stated that "the elements of established actions for 'monopolization' and 'attempted monopolization' are vital to differentiate between efficient and natural monopolies on the one hand, and unlawful monopolies on the other."[42] "*Berkey Photo*'s monopoly leveraging doctrine fails to differentiate properly among monopolies."[43] The Eleventh Circuit addressed this issue as follows: "*Berkey Photo* [does not] extend to a situation in which a monopolist projects its power into a market it not only does not seek to monopolize, but in which it does not even seek to compete."[44] Furthermore, the Eleventh Circuit stated that the use of a position in one market to gain an advantage in another market is not an illegal market restraint unless "a significant fraction of buyers or sellers are frozen out of a market."[45] Thus, the district court's decision was in direct conflict with Eleventh Circuit precedent.[46] In addition, the Federal Circuit concluded that the district court apparently based its decision on a per se theory of *future* Sherman Act violation; however,

37. *Id.* at 1359.

38. *See id.*

39. *Id.* at 1359 (citing Twin Lab., Inc. v. Weider Health & Fitness, 900 F.2d 566 (2d Cir. 1990)).

40. *See Intergraph,* 195 F.3d at 1359-60.

41. *Id.* at 1360 (citing Fineman v. Armstrong World Indus., Inc., 980 F.2d 171 (3d Cir. 1992)).

42. *Id.* (citing *Alaska Airlines*, 948 F.2d at 548-49).

43. *Id.* (citing *Alaska Airlines*, 948 F.2d at 548-49).

44. *Id.* (citing Aquatherm Indus., Inc. v. Florida Power & Light Co. 145 F.3d 1258, 1262 (11th Cir. 1998)).

45. *Id.* (quoting Amey, Inc. v. Gulf Abstract & Title, Inc. 758 F.2d 1486, 1503-04 (11th Cir. 1985)).

46. *See Intergraph,* 195 F.3d at 1360.

the Federal Circuit rejected this unwarranted "enlargement of antitrust theory and policy to prohibit downstream integration by a monopolist into new markets."[47]

D. Coercive Reciprocity and Tying

Fourth, the district court erred in finding that Intel engaged in unlawful "coercive reciprocity," defined by the district court as "the practice of using economic leverage in one market coercively to secure competitive advantage in another," by its proposals to settle the patent disputes.[48] "To violate the Sherman Act the entity that coerces reciprocal dealing must be a monopolist in one product and thus be positioned to require dealing in the coerced product, which but for the monopolist's coercion could be acquired elsewhere."[49] For example, in *Betaseed, Inc. v. U&I Inc.*, Betaseed excluded competition in the market for beet seeds because it was "the only processor of sugar beets geographically accessible to the U & I company," and it would only process beets grown from Betaseed's seeds.[50]

Unlike *Betaseed*, Intel's licensing proposals furthered no illegal relationship.[51] Intel did not demand that Intergraph buy its products, and the record described no market in which Intel's licensing proposals were shown to have distorted competition.[52] The Federal Circuit noted that the district court failed to explain its holding that Intel's proposal to trade a license for the Clipper patent in exchange for continuation of the "strategic customer" program violated both sections 1 and 2 of the Sherman Act.[53] The district court failed to set forth the following necessary elements under sections 1 and 2 of the Sherman Act: (1) "specific intent to monopolize;" (2) conduct that threatens actual monopolization; and (3) "harm to competition."[54]

Moreover, "[c]ommercial negotiations to trade patent property rights for other consideration in order to settle a patent dispute is neither tying nor coercive reciprocity in violation of the Sherman

47. *Id.* at 1360.

48. *Id.* at 1360-61.

49. *Id.* at 1361.

50. *Id.* (citing Betaseed, Inc. v. U&I Inc., 681 F.2d 1203, 1216 (9th Cir. 1982)). *See* Spartan Grain & Mill Co. v. Ayers, 581 F.2d 419 (5th Cir. 1978).

51. *Id.* at 1361.

52. *See Intergraph*, 195 F.3d at 1361.

53. *See id.* The Sherman Act does not require parties to bargain as equals.

54. *Id.*

Act."[55] Therefore, the Federal Circuit found that the district court erred in ruling that Intel's activities violated sections 1 and 2 of the Sherman Act under the theories of coercive reciprocity and tying.[56]

E. Use of Intellectual Property to Restrain Trade

The Federal Circuit further held that the district court erred in finding that Intel was using its intellectual property to restrain trade; specifically, the district court incorrectly rejected Intel's argument that its proprietary information and pre-release products were subject to copyright and patent protection.[57] The antitrust laws do not negate the patentee's right to exclude others from patent property.[58] To wit, "[a] patent holder who lawfully acquires a patent cannot be held liable under Section 2 of the Sherman Act for maintaining the [monopoly] power he lawfully acquired by refusing to license the patent to others."[59]

The Federal Circuit noted that, in supporting its finding that Intel was using its intellectual property to restrain trade, the district court relied on the proposition that "[u]nlawful exclusionary conduct can include a monopolist's unilateral refusal to license a [patent or] copyright or to sell a patented or copyrighted work."[60] However, the district court apparently misconstrued the teachings of the Ninth Circuit. In effect, the Ninth Circuit developed the following rebuttable presumption: "'while exclusionary conduct can include a monopolist's unilateral refusal to license a [patent or] copyright,' or to sell its patented or copyrighted work, a monopolist's 'desire to exclude others from its [protected] work is a presumptively valid business justification for any immediate harm to consumers.'"[61] Furthermore, the "Ninth Circuit . . . found 'no reported case in which a court imposed antitrust liability for a unilateral refusal to sell or license a patent or copyright.'"[62] Similarly, the Federal Circuit found

55. *Id.* at 1362.

56. *Id.* at 1361.

57. *See id.* at 1362.

58. *See Intergraph*, 195 F.3d at 1362. *See also* Cygnus Therapeutics Sys. v. ALZA Corp., 92 F.3d 1160 (Fed. Cir. 1996).

59. *Id.* at 1362-63 (citing Miller Insituform, Inc. v. Insituform of N. Am., Inc., 830 F.2d 606, 609 (6th Cir. 1987)).

60. *Id.* at 1362 (citing Image Technical Services, Inc. v. Eastman Kodak Co., 125 F.3d 1195, 1218 (9th Cir. 1997)).

61. *Image Technical Services*, 125 F.3d at 1218 (quoting *Data Gen. Corp.*, 36 F.3d at 1187).

62. *Id.* at 1216.

no such antitrust liability in this case.[63]

The Federal Circuit then noted that what was at issue before the district court was not licenses to Intel's patents and copyrights; rather, Intergraph sought a preferred position as to the products that embody this intellectual property before they are commercially available, as well as access to trade secrets.[64] Even though a key intellectual property right at issue was trade secrets and not copyrights or patents, the Federal Circuit had no difficulty holding that "the owner of proprietary information has no obligation to provide it, whether to a competitor, customer, or supplier."[65] Thus, "a customer who is dependent on a manufacturer's supply of a component can not [sic] on that ground force the producer to provide it; there must also be an anticompetitive aspect invoking the Sherman Act."[66] In sum, the Federal Circuit found no antitrust liability under a use of intellectual property to restrain trade theory.

F. Breach of Contract

Finally, the Federal Circuit found that the district court also based its grant of injunction on a contract theory.[67] Here, the district court cited a letter from Intel to Intergraph stating that Intergraph would be treated as "a strategic customer in present and future programs" that are "currently being managed under Non-Disclosure Agreements."[68] The Federal Circit rejected this alternative basis for the injunction, focusing on the total lack of detail in the supposed contract.[69] Specifically, the court set forth the following:

> [T]he letter's broad usages, its lack of specificity, and its silence on virtually all of the elements of a contract, negate its interpretation as replacing the non-disclosure agreements with specific obligations, and separate it from the sort of document subject to a "gap-filler" expedient. There [was] no gap-filling exercise that can reasonably include all of the terms of the district court's injunction

63. *See Intergraph*, 195 F.3d at 1362 (quoting *Image Technical Services*, 125 F.3d at 1216). *See* CSU, L.L.C. v. Xerox Corp., 203 F.3d 1322 (Fed. Cir. 2000) (holding that Xerox was under no obligation to sell or license its patented parts or its copyrighted works and did not violate the antitrust laws by refusing to do so).

64. *See Intergraph*, 195 F.3d at 1363.

65. *Id.*

66. *Id.*

67. *See id.* at 1366.

68. *Id.* (citing *Intergraph*, 3 F. Supp. 2d at 1267).

69. *See id.*

order.[70]

III. CONCLUSION

In sum, the Federal Circuit held that the antitrust rulings of the district court were incorrect in law or were devoid of sufficient factual support to present a substantial likelihood of establishing an antitrust law violation with respect to the issues presented.[71] This decision reinforces the well-established proposition, ignored by the district court, that the mere presence of monopoly power is not actionable; a successful antitrust claim requires harm to competition.

Likewise, this decision is support for the proposition, repeatedly championed by the Federal Circuit but open to some question in the Ninth Circuit, that the exercise of rights inherent in intellectual property will rarely, if ever, lead to antitrust liability.

70. *Intergraph*, 195 F.3d at 1366 (citing ALA. CODE §§ 7-2-305 to -310 (1965)).

71. *See Intergraph*, 195 F.3d at 1352.

WANG LABORATORIES, INC. v. AMERICA ONLINE, INC. AND NETSCAPE COMMUNICATIONS CORP.

Daniel R. Harris[†] and Janice N. Chan[††]

I. BACKGROUND

The explosion of business method and software patents, particularly those addressing Internet technologies, has generated significant analysis focused on how the Patent and Trademark Office ("PTO") evaluates such applications. Many have criticized the PTO for issuing patents on such fundamental concepts as using credit cards securely on-line;[1] using electronic "shopping carts" on-line;[2] allowing on-line purchase through one click of a mouse;[3] and using on-line affiliate programs to promote a web site.[4] In response, the PTO recently announced a plan for increasing the scrutiny of business method patent applications before they are granted.[5] The question remains, however: What about the thousands of patents that have already issued?

While the press has given a great deal of attention to how these patents are approved by the PTO, it has virtually ignored how courts have interpreted the patents after they issue. Judicial interpretation of patent claims, commonly referred to as claim construction, appears to be the next battleground in the fight over Internet patents. The Federal Circuit's recent analysis in *Wang Laboratories, Inc. v. America Online, Inc. and Netscape Communications Corp.*[6] provides some indication that courts will look to interpret Internet patent

---

[†] Daniel R. Harris is a partner in the Intellectual Property Group at Brobeck Phleger & Harrison, LLP, resident in Brobeck's Palo Alto, California office.

[††] Janice N. Chan is a J.D. Candidate 2000 at Santa Clara University, School of Law. Janice would like to thank David Banie, Traci Pickering, Barrett Schaefer and Jennifer Ishimoto for their help with this case note. Janice can be reached at jc0812@hotmail.com.

1. U.S. Pat. No. 5,724,424 to Gifford.
2. U.S. Pat. No. 5,715,314 to Payne et al.
3. U.S. Pat. No. 5,960,411 to Hartman et al.
4. U.S. Pat. No. 6,029,141 to Bezos et al.
5. *See Business Methods Patent Initiative: An Action Plan* (visited Apr. 17, 2000) <http://www.uspto.gov/web/offices/com/sol/actionplan.html>.
6. 197 F.3d 1377 (Fed. Cir. 1999).

claims narrowly in an effort to control the impact on future innovation.

The Federal Circuit rejected Wang Laboratories, Inc.'s ("Wang") appeal of a holding by the United States District Court for the Eastern District of Virginia granting summary judgment of noninfringement for defendants America Online, Inc. ("AOL") and Netscape Communications Corp. ("Netscape").[7] Wang's underlying suit alleged infringement of its U.S. Patent No. 4,751,669 ("'669 patent")[8] covering, among other things, AOL's and Netscape's respective Internet browser "bookmark" functions. The '669 patent, entitled "Videotex Frame Processing," teaches an on-line information system that provides users with both textual and graphical information from computer-controlled databases through interactive two-way communication over a telephone network. Interpreted broadly, the Wang Videotex patent could apply to a myriad of modern Internet web sites and browsers.

At trial, Wang asserted numerous claims against AOL and Netscape. On appeal, Wang emphasizes infringement of claims 20 and 38. Wang asserts that Claim 20 is infringed by AOL's "favorite places" and Netscape's "bookmark" features. Claim 20 is essentially a keyword feature that allows the user to assign a name to a certain page or frame and thus allows for easy retrieval:

> 20. Apparatus for retrieving selected frames of information from a central videotex supplier of the information frames, each information frame having an associated unique identifier assigned by the supplier for retrieving the frame, the apparatus comprising a display device connected to display the information frames, storage means connected to store the identifier and a unique keyword selected by an operator and associated with the identifier, menu means connected to display on the display device a menu frame containing the keyword, data entry means connected to enter into the apparatus a request for retrieval of a selected information frame by moving a cursor to the keyword associated with the selected information frame, and a processor connected to be responsive to the data entry means for retrieving the information frame in response to the entry of the request by transmitting the associated identifier to the supplier.[9]

Wang's other major allegation addresses its patent Claim 38

---

7. *See id.*
8. U.S. Pat. No. 4,751,669 to Sturgis et al.
9. *Wang*, 197 F.3d at 1379.

which describes the feature of tagging a stored page or frame in order to identify and activate the decoding protocol when information is retrieved. Claim 38's structural components are presented in means-plus-function form:

> 38. Apparatus for locally processing frames of information received from central videotex suppliers, different frames being encoded in accordance with different protocols, comprising means connected to locally store the information frames, means connected to locally display the frames, means connected to decode the locally stored frames as they are displayed, and means connected to tag each stored frame with a header indicating one of said different protocols as having been used for encoding the frame, the means connected to decode being arranged to decode each frame in accordance with the protocol indicated by the header on the frame.[10]

Several protocols for processing and displaying computer-generated data were already in existence at the time the '669 patent was granted. The two general types of these protocols are character-based protocols and bit-mapped protocols. It is not disputed that both AOL and Netscape used bit-mapped protocols.[11]

In granting summary judgment of noninfringement in favor of defendants Netscape and AOL, the district court ruled that all of the claims asserted by Wang were limited to character-based protocols. This holding followed from the court's definition of the term "frame" as used in the Wang patent as a "page of information assembled prior to display which is encoded in a character-based protocol . . . to then be displayed on the screen representing a fixed full screen arrangement, such as rows and columns, of alphanumeric and graphic characters."[12]

Thus, by limiting the term "frame" to those pages of information encoded in a character-based protocol, the district court found no infringement because the AOL and Netscape products used a bit-mapped protocol.[13]

II. HOLDING, RATIONALE AND DISCUSSION

On appeal, the Federal Circuit agreed with the district court and

10. *Id.*

11. *See id.*

12. *Id.*

13. *See id.* at 1380 (citing the lower court's decision in Wang Labs v. America Online, Inc., No. Civ. A. 97-1628-A, 1998 WL 1157608 (E.D. Va. May 1, 1998)).

held that the term "frame" as used in the patent was limited to pages encoded in character-based protocols.[14] The Court of Appeals further concluded that the bit-mapped protocols were not equivalent to character-based protocols for the purpose of the patent's means-plus-function claims, and that the patent was not infringed under the doctrine of equivalents.[15]

A. Claim Construction

Wang argued for a broader construction of the claims by focusing on two points: (1) the term "frame," as used in the '669 patent should encompass both character-based and bit-mapped protocols;[16] and (2) even if the patent's specification is deemed to be limited to character-based protocols, that the interchangeability of character-based and bit-mapped information protocols was known at the time the '669 invention was made.[17]

In support of its first point, Wang argued that the term "frame" as used in the patent referred broadly to a "unit of digital data that could be selected and displayed,"[18] and thus should not be limited to the use of a character-based protocol. Thus, Wang argued that the display of "alphanumeric and graphic characters"[19] included both character-based and bit-mapped displays. AOL and Netscape refuted Wang's argument by reasoning that the usage of the term "frame" in conjunction with the term "characters" limited the invention to a character-based protocol.[20] In support of this argument, AOL and Netscape pointed out that the '669 specification used the term "frame" only with respect to a character-based protocol.[21]

The Federal Circuit, in concluding that the term "frame" as used in the '669 claims did not encompass a more general usage of both bit-mapped and character-based protocols, reasoned that "the only system that is described and enabled in the '669 specification and drawings uses a character-based protocol."[22] The court concluded that, while the specification does mention non-character-based protocols, these references to bit-mapped protocols were mere

14. *See id.* at 1382.
15. *See Wang*, 197 F.3d at 1377.
16. *See id.* at 1381.
17. *See id.* at 1383.
18. *Id.* at 1381.
19. *Id.*
20. *See id.*
21. *See Wang*, 197 F.3d at 1381.
22. *Id.* at 1382.

acknowledgments of the state of the art and not a broadening of the invention of the patent.[23]

To support its second point, Wang argued that even if the specification is deemed to encompass only character-based protocols, the claims themselves should not be so limited because the interchangeability of character-based and bit-mapped protocols was known at the time the '669 invention was created.[24] Wang argued that the user interface features of the claims is the core invention of the '669 patent, not the choice of protocol.[25] AOL and Netscape pointed to the patent specification and suggested that it was directed, and thus limited, to interactions based on character-based information frames and that this limitation was the basis for the subsidiary features of keywords.[26]

On this second issue, the Federal Circuit once again affirmed the district court and found in favor of AOL and Netscape.[27] The Court ruled that the "claims were not directed solely to the user interface, but to the electronic system that is described as implementing this interface."[28]

B. Preferred Embodiment

Wang next argued that the character-based protocol was merely a "preferred embodiment," and as such, the embodiment as described in the specification does not set the boundaries of the claims. Wang argued that "limitations from the specification are not to be read into the claims."[29]

AOL and Netscape countered that when the subject matter claimed is the only one contained in the specification, then the invention is so limited and not simply a "preferred" example of a broader undefined invention.[30] AOL and Netscape cited *Modine Mfg. Co. v. United States Int'l Trade Comm'n*,[31] in which the court ruled "when the 'preferred embodiment' is described as the invention itself,

23. *See id.*
24. *See id.*
25. *See id.*
26. *See id.*
27. *See Wang*, 197 F.3d at 1383.
28. *Id.*
29. *Id.* (citing Comark Communications, Inc. v. Harris Corp., 156 F.3d 1182, 1186 (Fed. Cir. 1998)).
30. *See id.*
31. 75 F.3d 1545 (Fed. Cir. 1996).

the claims are not entitled to a broader scope than that embodiment."[32]

The Federal Circuit agreed with AOL and Netscape, ruling that the "preferred" usage itself does not broaden the claims beyond their specifications.[33] The court held that, because the '669 specification only describes the character-based protocol embodiment, the district court was correct in thus limiting the interpretation of Wang's claim.[34]

C. Means-Plus-Function Claims

Wang further argued that under 35 U.S.C. § 112, ¶ 6 the "means" are not limited to the character-based protocol as described in the specification and that a known bit-mapped protocol is an equivalent means, interchangeable with the character-based protocol.[35] Thus, Wang argued that if the claimed function is adequately described in the specification, then an equivalent structure under 35 U.S.C. § 112, ¶ 6 need not be described in the specification.[36] Under this argument, the known bit-mapped protocol would not need to be included in the specification in order to be equivalent under 35 U.S.C. § 112, ¶ 6.[37]

AOL and Netscape argued that even though the character-based and bit-mapped modules performed similar functions, their capabilities and methods of operation were so different that they were not "equivalent" under 35 U.S.C. § 112, ¶ 6.[38] AOL and Netscape pointed out that the capabilities were so different that Wang's scientists were unable to implement bit-mapped technology in their system: "Wang's inability to implement bit-mapped technology should not be rewarded with a judgment of equivalency after others later succeeded."[39]

Once again, the Federal Circuit agreed with the defendants, holding that the evidence supported the district court's ruling of non-equivalency under 35 U.S.C. § 112, ¶ 6.[40] Further, the court noted expert testimony demonstrating that, though the protocols are interchangeable today, they function on very different principles and

---

32. *Id.* at 1551.

33. *See Wang*, 197 F.3d at 1383 (citing General American Transp. Corp. v. Cryo-Trans, Inc., 93 F.3d 766 (Fed. Cir. 1996)).

34. *See id.*

35. *See id.* at 1385.

36. *See id.*

37. *See id.*

38. *See id.*

39. *Wang*, 197 F.3d at 1385.

40. *See id.*

have different capabilities.[41] In addition, the '669 inventors testified that Wang had stopped development of the bit-mapped protocol in their system, in part, because they were having technical difficulties.[42] Thus, the court held that the bit-mapped protocol was not equivalent under 35 U.S.C. § 112 ¶ 6.[43]

D. Claim Differentiation and the Doctrine of Equivalents

The court also ruled against Wang on its argument under claim differentiation.[44] The court ruled that the claim differentiation argument in and of itself does not support interpreting the term "frame" as applicable to any protocol.[45]

Wang argued that the doctrine of equivalents, under which a known equivalent need not be described in the specification, applies to both character-based and bit-mapped protocols because they are interchangeable.[46] However, the court ruled that no reasonable trier of fact could find substantially the same function between the '669 patent and the accused systems because of the great differences in operation, structure, and capabilities.[47]

III. LIMITATIONS ON BUSINESS METHOD PATENTS

Although Wang sought broad coverage from its patent, the district court and Federal Circuit both interpreted Wang's claims narrowly so as to find noninfringement. As courts address more and more actions in which Internet patent claims are asserted broadly, judicial claim construction will emerge as a means of restricting their impact. Although patent holders may assert broad claims against the industry, individual defendants should scour the patent specification for language restricting its application.

The Legislature appears to be heading in the same direction as well. For example, Congress has also taken part in this trend of narrowing the scope of business method patents by passing the First

41. *See id.*

42. *See id.*

43. *See id.*

44. *See id.* at 1384.

45. *See Wang*, 197 F.3d at 1384.

46. *See id.* at 1386. "[K]nown interchangeability" is a useful objective standard of equivalency. *See* Warner-Jenkinson Co. v. Hilton Davis Chem. Co., 520 U.S. 17 (1997).

47. *See Wang*, 197 F.3d at 1386.

Inventor Defense Act of 1999,[48] which introduced a defense to an action for infringement with respect to method claims. Section (a)(3) of this statue narrowly defined the term "method" as "a method of doing or conducting business," which effectively limits this defense to business method patents.[49] This legislation was apparently motivated by the Federal Circuit's recent decision in *State Street Bank & Trust v. Signature Financial Group*, which held that methods for doing business are patentable.[50] The legislators believed that "[t]he *State Street* court came down on the side of a very broad scope of subject matter that qualifie[d] for patent protection."[51] To wit, "*State Street* clarifie[d] that the characterization of subject matter as a method of doing business [did] not render it unpatentable."[52]

In response to the *State Street* decision, Congress set forth this defense in order to protect holders of trade secrets in light of the "increase in the ability to patent all business methods and processes."[53] Congress noted that "[t]housands of 'back-office' processes are now being patented."[54] Previously, the businesses that developed these processes thought that secrecy was the only protection available.[55] "Under established law, these pre-existing processes do not now qualify for patent protection because they have been in commercial use."[56] Therefore, Congress introduced this legislation in order to "clarif[y] the interface between two key branches of intellectual property law–patents and trade secrets."[57]

Even those companies actively seeking their own Internet-focused business method patents have expressed concern about their impact on the industry. In an open letter, for example, Amazon.com

---

48. 35 U.S.C.A. §273 (West Supp. 2000). Specifically, § 273 provides that:

> It shall be a defense to an action for infringement under section 271 of this title with respect to any subject matter that would otherwise infringe one or more claims for a method in the patent being asserted against the person, if such person had, acting in good faith, actually reduced the subject matter to practice at least 1 year before the effective filing date of such patent, and commercially used the subject matter before the effective filing date of such patent.

Id.

49. *Id.*

50. *See* H.R. No. 106-287(I), 106th Cong., 1st Sess. (1999) (citing State Street Bank & Trust v. Signature Fin. Group, 149 F.3d 1368 (Fed. Cir. 1998)).

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.*

55. *See id.*

56. H.R.No. 106-287 (I).

57. *Id.*

CEO Jeff Bezos recently suggested that business method and software patents should have a shorter lifespan of three to five years rather than the current seventeen years.[58] In addition, Bezos proposed a short comment period during which the public could provide prior art references to patent examiners prior to issuance of the proposed patent.[59]

IV. CONCLUSION

The analysis affirmed by the Federal Circuit in *Wang* may embolden other district courts to interpret claims narrowly. Employing narrow claim construction, as the Federal Circuit did in *Wang*, courts can end litigation with a finding of noninfringement at the summary judgment stage. While the Legislature and the PTO work to modify the patent system to reduce the number of weak business method patents being issued, narrow claim construction may prove to be a powerful argument for defendants to argue against the application of broadly asserted patents in court.

58. *See* Open letter from Jeff Bezos, CEO, Amazon.com (on file with the *Santa Clara Computer and High Technology Law Journal*).

59. *See id.*

LEGISLATIVE NOTE: RECENT STATE LAWS REGULATING UNSOLICITED ELECTRONIC MAIL

Max P. Ochoa[†]

I. INTRODUCTION

This Note surveys recent state laws enacted in response to unsolicited electronic mail or "spam."[1] Unsolicited electronic mail is perceived by many users of the Internet and the Worldwide Web as a nuisance. Other authors have described the economic incentives for, and the infrastructural costs associated with, spam.[2] More seriously, spam may be an obstacle to the success of the Internet economy.[3] While the U.S. Congress has been slow to act,[4] state legislatures have been far more responsive. Since the first bill was introduced in the

---

[†] Max P. Ochoa is an associate in the Information Technology group of Cooley Godward LLP. Mr. Ochoa holds a B.S. from the Massachusetts Institute of Technology, an M.S. from the University of Michigan, and a J.D. from Stanford Law School. Mr. Ochoa would like to thank Eric Goldman, Jennifer Ulveling for their assistance in the preparation of background materials for this Note, and Lisa Sternoff in skillfully shepherding him through the editing process. However, Mr. Ochoa states that any errors or omissions are his own.

1. Unsolicited electronic mail is known by many names, including "unsolicited bulk email," "unsolicited commercial email," or UCE, and spam. In this Note, "unsolicited electronic mail" and "spam" will be the preferred names.

2. *See, e.g.*, Lisa M. Sternoff, Comment, *Taking Spam Out of the American Diet* (Feb. 1999) (unpublished comment, text available online at <http://www.lisasternoff.com>); Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 BERKELEY TECH. L.J. 233, 276 (1996); Barry Bowern, *Controlling unsolicited bulk e-mail: Who's taking action? What's being done?* SUNWORLD (Aug. 1997) <http://www.sunworld.com/swol-08-junkemail.html>.

3. *See, e.g.*, Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, AT&T LABS-RESEARCH TECHNICAL REPORT TR 99.4.3 (Apr. 14, 1999) <http://www.research.att.com/projects/privacystudy> (documenting Internet users' concerns regarding, *inter alia*, receiving unsolicited communications as a result of their on-line activities).

4. As of March 2000, the U.S. Congress is considering nine different bills addressing unsolicited electronic mail. Eight bills were introduced in the 105th Congress, none of which became law. For a detailed list of pending legislation, see CAUCE, Coalition Against Unsolicited Commercial Email (visited Mar. 28, 2000) <http://www.cauce.org>.

Nevada senate in January 1997,[5] fourteen states have passed sixteen laws regulating spam, and four states created committees charged with addressing a host of Internet related issues, among them, spam.[6]

In enacting spam legislation, states have adopted a variety of approaches have been implemented by the states in the new laws, exemplifying Justice Brandeis' observation that the state may "serve as a laboratory; and try novel social and economic experiments."[7] Nonetheless, general patterns in the enacted legislation are emerging. Section II of this Note describes these general patterns and highlights a few notable exceptions from the trends.

As companies strive to get attention on the web, many are turning to consumers' inboxes.[8] In practice, it is difficult for anyone to know the physical location of the recipient only from an individual's e-mail address.[9] As a result, companies interested in exploiting the economic efficiencies of unsolicited electronic mail, but wanting to comply with the various state laws, must comply with the superset of the various state laws.[10] Section III describes "best practices" to be used by companies trying to minimize their exposure under the spam laws.

Section IV describes some shortcomings of the current laws, both legal (constitutionality and enforceability) and practical (effectiveness and ease of use by recipients of spam), and makes suggestions for improvements. Section V presents a very brief discussion of two recent decisions, one declaring Washington State's law unconstitutional under the "Dormant Commerce Clause," and another rejecting a summary judgement motion seeking to declare Louisiana's statute unconstitutional. Section VI concludes the Note.

---

5. NEV. REV. STAT. § 41 tit. 3 (1998) (introduced Jan. 1997, enacted July 1997, effective July 1, 1998).

6. Maine, Maryland, New Jersey and Oregon.

7. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1931) (Brandeis, J., dissenting).

8. An "inbox" is the electronic equivalent of a mailbox, where a user may see the electronic messages, solicited and unsolicited, that have been sent to the e-mail address associated with that inbox.

9. For example, maxochoa@yahoo.com alone, does not indicate that I am a resident of the State of California, or of the United States, for that matter.

10. In truth, the problem is far more vexing. As non-U.S. jurisdictions pass legislation regulating spam, a sender may need to worry about complying with the superset of all laws, foreign and domestic.

II. *LEITMOTIFS*[11] IN STATE LAWS REGULATING SPAM

As of March 3, 2000, fourteen states have passed sixteen laws regulating spam.[12] Additionally, the legislatures of four states[13] have formed committees charged with exploring legislative approaches to control spam. A review of the various statutes reveals that there are certain trends in the legislative efforts to date.

The laws can be divided into explicit unsolicited electronic mail regulation statutes and consumer protection statutes. Within each of these two broad categories of laws, there are many elements or legislative *leitmotifs* that can be seen at play.

A. Express Unsolicited Electronic Mail Statutes

These are statutes that attempt to define unsolicited commercial e-mail and to regulate it. A typical definitional scheme is that of North Carolina: "'Unsolicited' means not addressed to a recipient with whom the initiator has an existing business or personal

---

11. *Leitmotifs* are melodic passages or phrases in music, Wagnerian opera in particular, that represent a character or emotion. *Leitmotif* may also refers to a dominant and recurring theme or pattern, and that is the sense in which it is used in this Note.

12. In order of date of effectiveness of the laws, the states that have enacted spam regulations are:

Washington, WASH. REV. CODE § 19.190 (1998) (effective June 11, 1998, *as amended* by H.B. 1037 (Wash. 1999), *declared unconstitutional* in State v. Henckel. *See* Section V, *infra.* note 40);

Nevada, NEV. REV. STAT. §§ 41.705-.735 (1998) (effective July 1, 1998);

California, CAL. BUS. & PROF. CODE § 17538.4 (1999) and §17538.45 (1999) (both effective Jan. 1, 1999);

West Virginia, W. VA. CODE § 46a-6G-1 *et seq.* (1999) (effective June 11, 1999);

Tennessee, TENN. CODE ANN. §§ 47-18-2501, -2502 (1999) (effective June 17, 1999);

Iowa, IOWA CODE § 714D (1999) (effective July 1, 1999);

Oklahoma, OKLA. STAT. Tit. 15, § 776.1 *et seq.*, Tit. 74, § 5060.52 (1999) (effective July 1, 1999);

Virginia, VA. CODE ANN. §§ 8.01-328.1, 18.2-152.2, -152.4, -152.12 (1999) (effective July, 1, 1999);

Delaware, DEL. CODE ANN. tit. 11, §§ 936-941 (1999) (effective July 2, 1999);

Rhode Island, R.I. GEN. LAWS § 6-47 (1999) (effective July 8, 1999) and §§ 11-52-1, -6, -4.1 (1999) (effective Oct. 1, 1999);

Louisiana, LA. REV. STAT. §§ 14:73.1(5), (8), (12), (13), 14:73.6 (1999) (effective Aug. 15, 1999);

Connecticut, 1999 Conn. Acts 99-160 (Reg. Sess.) (effective Oct. 1, 1999, *also repealing and substituting* CONN. GEN. STAT. § 52-59(b)) CONN. GEN. STAT. §§ 42 *et seq.*, 52-59(b) (1999) (effective Oct. 1, 1999)];

North Carolina, N.C. GEN. STAT. §§ 1-75.4, 14-453, 14-458, 1-539.2a (1999) (effective Dec. 1, 1999);

Illinois, 815 ILL. COMP. STAT. 511/1 *et seq.* (1999) (effective Jan. 1, 2000).

13. *See supra* note 6.

relationship and not sent at the request of, or with the express consent of, the recipient."[14] "'Commercial electronic mail" means messages sent and received electronically consisting of commercial advertising material, the principal purpose of which is to promote the for-profit sale or lease of goods or services to the recipient."[15]

B. Consumer Protection Statutes

These laws are arguably the easiest with which to comply. In general, the only requirements on spam are that no misleading subject lines be used and that the sender of the e-mail not alter or misrepresent or obfuscate the so-called header (information describing the route the e-mail has taken through the Internet from sender to recipient) of the e-mail. The intent of the laws is not to prevent spam, but rather to make spammers be "honest" in the subject lines of their e-mails and for their e-mails to be traceable.

Provided, if one complies with these requirements, one can send as much spam as one likes. These statutes are generally codified along with other consumer protection provisions of the particular state.

C. Additional Legislative Leitmotifs

1. Spam Software Prohibitions

Beginning with Virginia, several states seek to prohibit software that facilitates spam.[16] Because software can be speech, it is likely that these provisions of the statutes will be found to violate the First Amendment.[17]

---

14. N.C. GEN. STAT. §§ 14-453(10) (1993).

15. N.C. GEN. STAT. §§ 14-453(1b) (1999).

16. *See, e.g.*, VA. CODE ANN. §§ 18.2-152.4(b) (1999):

> It shall be unlawful for any person knowingly to sell, give or otherwise distribute or possess with the intent to sell, give or distribute software which (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.

17. *See* Junger v. Daley, 2000 WL 343566, *4 (6th Cir. 2000). Justice Martin wrote: "Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment." See *also* Bernstein v. U.S. Department of Justice, 176 F.3d 1132 (9th Cir. 1999), *reh'g granted,*

2. Long Arm Statutes

While the judicial framework of jurisdiction is being crafted case-by-case, several state legislatures have attempted to assist judges' traditional personal jurisdiction analysis by explicitly amending their long-arm statutes to contemplate the sending of spam into their state from outside the state.[18] This is an obvious benefit to plaintiffs, who may be spammed from beyond the borders of their home state.

3. ISP Safe Harbors

All states which have passed spam laws have created safe harbors for Internet service providers, or ISPs. ISPs are companies that provide individuals with connectivity and bandwidth to the Internet. States have created two forms of ISP safe harbors. The first is the safe harbor for the transmission of spam. In every state regulating spam, with the notable exception of Louisiana, an ISP cannot be held liable for a violation of the spam laws because it simply transmitted spam-encoding packets.[19] About half the states have created a second type of safe harbor, shielding ISPs from liability for attempting to prevent spam.[20] Left unanswered by the statutes is the question of vicarious liability of an ISP that knowingly allows spam to be sent through its servers.

---

withdrawn, 192 F.3d 1308 (9th Cir. 1999), where the court found that not even the Government's strong interest in preventing the proliferation of strong encryption code, surely more compelling than the state's interest in preventing spam, could limit the free speech inherent in the creation of software.

18. *See, e.g.*, OKLA. STAT., Tit. 15, § 776.3 (1999): "Transmitting or causing the transmission of fraudulent electronic mail to or through a computer network of an electronic mail service provider located in this state shall constitute an act in this state."

19. *See, e.g.*, W. VA. CODE § 46a-6G-3(4) (1999): "No interactive computer service or public utility will be liable for merely transmitting a bulk electronic mail message on its network."

20. *See, e.g.*, W. VA. CODE § 46a-6G-3(1)-(3) (1999):

> (1) An interactive computer service may block the receipt or transmission through its service of any bulk electronic mail that it reasonably believes is, or will be, sent in violation of this article.
>
> (2) An interactive computer service may disconnect or terminate the service of any person that is in violation of this article.
>
> (3) No interactive computer service may be held liable for any action voluntarily taken in good faith to block the receipt or transmission through its service of any bulk electronic mail which it reasonably believes is, or will be, sent in violation of this article; nor will any interactive computer service be held liable for any action voluntarily taken in good faith to disconnect or terminate the service of any person that is in violation of this article.

4. Civil or Criminal Remedies; Who Can Seek Them?

The states have varied significantly in defining the potential plaintiff and in choosing whether or not to criminalize a violation of the spam law. States have variously given rights of action to one or more of the following: ISPs, individual recipients of the spam and the state attorney generals. Some states have made violations civil offenses and others have criminalized violations, with the most flagrant or repeated violations categorized as a felony with prison terms of several years.

D. Exceptions

Some state statutes do not limit themselves to commercial e-mails.[21] This raises clear constitutionality concerns as government regulations of non-commercial speech faces stricter scrutiny than does regulation of commercial speech.[22] However, to the extent these laws are addressing false advertising or fraudulent behavior, and arguably, the use of misleading subject lines and the misrepresentation of the origin or routing path of an electronic message constitute such behavior, the constitutionality question is not reached in the first instance.

III. "BEST PRACTICES" FOR MINIMIZING EXPOSURE TO STATE SPAM LAWS

If a sender could somehow know that all her intended unsolicited electronic mail recipients are in Louisiana, then she only need worry about complying with the Louisiana statute. As stated in the introduction, it is very difficult for a sender of an e-mail to know with any certainty where that e-mail will be received. In effect, an e-mail

21. Virginia, West Virginia, Oklahoma, Connecticut, and Rhode Island's statutes are illustrative of this point.

22. Supreme Court jurisprudence on the First Amendment is vast and complex. However, speaking broadly, the Supreme Court has held that content-based restrictions on speech are presumptively unconstitutional and that in order for such restrictions to be upheld, the government must show that the regulation is necessary to serve a compelling state interest and it is narrowly tailored to achieve that end, a level of judicial review commonly referred to as *strict scrutiny*. *See, e.g.*, Simon & Schuster, Inc. v. Members of the New York State Crime Victims Board, 502 U.S. 105 (1991). State restrictions on commercial speech are subject to somewhat greater deference from the courts, though false advertising is not protected by the First Amendment. After determining if the commercial speech addresses a lawful activity and is not misleading or fraudulent, a court will uphold a regulation on commercial speech if the regulation serves a substantial governmental interest, it directly advances that interest, and is narrowly tailored to serve the substantial interest. *See, e.g.*, Board of Trustees of State University of New York v. Fox, 492 U.S. 469 (1989).

sender who desires to comply with, or at least minimize her risk of violating, the various state spam laws must tailor her messages to comply with the superset of all the state laws.[23] This could be a daunting challenge. However, because of the general patterns outlined in Section II, it turns out that the task is manageable. The following are suggested "best practices" for minimizing one's risk of violating the state spam laws.[24]

Do not "spoof" header information. "Spoofing" header information is a practice used to conceal, obfuscate or misrepresent the origination point and routing information present in the header of most e-mail messages. The "header" of an e-mail message is a field of information found at the beginning or "head" of an e-mail message. The header identifies the origination point and routing information of a given e-mail address. By reviewing the header of an e-mail, one can trace it to its origin. Washington law provides a typical statutory prohibition:

> No person may initiate the transmission... of a commercial electronic mail message... that uses a third party's Internet domain name without permission of the third party, or otherwise misrepresents or obscures any information in identifying the point of origin or the transmission path of a commercial electronic mail message.[25]

Start subject lines with ADV: or ADV:ADLT. By starting the subject line of an unsolicited commercial e-mail with "ADV:" (or "ADV:ADLT" if the subject matter of the e-mail is intended for persons over 18 years of age), one will avail oneself of a safe harbor of the California, Tennessee and Rhode Island laws.[26]

Do not use misleading subject lines.[27] An example of a

---

23. *See supra* note 10.

24. It should be noted that this area of the law is in heavy flux, and that as new laws are added by the states or Congress, this advice may change.

25. WASH. REV. CODE § 19.190.020(1)(a) (1998).

26. *See, e.g.*, TENN. CODE ANN. §§ 47-18-2501(e) (1999):

> In the case of e-mail that consists of unsolicited advertising material for the lease, sale, rental, gift, offer or other disposition of any realty, goods, services or extension of credit, the subject line of each and every message shall include "ADV:" as the first four (4) characters. If these messages contain information that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, that may only be viewed, purchased, rented, leased, or held in possession by an individual eighteen (18) years of age or older, the subject line of each and every message shall include "ADV:ADLT" as the first eight (8) characters.

27. *See, e.g.*, NEV. REV. STAT. § 41-730(1)(c) (1998): "[I]f a person transmits or causes to

misleading subject line is "Great seeing you last week!". One expects to receive an enthusiastic e-mail from a friend. Instead, the e-mail is an unsolicited electronic mail. Arguably if one follows the prior suggestion, one will automatically comply with this statutory requirement of many of the laws. An example of an accurate subject line for a widget-monger might be "We are offering you a one-time special on widgets."

Establish a valid reply-to e-mail address or toll-free telephone number.[28] One must make it easy and cost-free for a recipient of one's unsolicited electronic mail to notify one that they do not wish to receive further e-mails.

Notify recipients of how they can request no further e-mails.[29] The first text in the body of the e-mail should describe the method that may be used by the recipient to request that no more e-mails be sent to her.[30] This can be a bitter pill to swallow for many people with sales and marketing responsibilities. They want the advertisement to be the first thing seen. While many senders of spam place the information on discontinuing further e-mails at the end of their messages, they are not complying with the letter of the law.

Do not send further e-mails to people who have requested to be removed from the distribution list.[31] Senders of unsolicited electronic mail must set up a mechanism to compare e-mail addresses

---

be transmitted to a recipient an item of electronic mail that includes an advertisement, the person is liable to the recipient for civil damages unless the advertisement is readily identifiable as promotional, or contains a statement providing that it is an advertisement . . . ."

28. *See, e.g.*, TENN. CODE ANN. §§ 47-18-2501(d) (1999): "[Sender shall] establish a toll-free telephone number or valid sender operated return e-mail address that the recipient of the unsolicited documents may call or e-mail to notify the sender not to e-mail any further unsolicited documents."

29. *See, e.g.*, CA. BUS. & PROF. § 17538.4(b) (1999):

> All unsolicited faxed or e-mailed documents subject to this section shall include a statement informing the recipient of the toll-free telephone number that the recipient may call, or a valid return address to which the recipient may write or e-mail, as the case may be, notifying the sender not to fax or e-mail the recipient any further unsolicited documents to the fax number, or numbers, or e-mail address, or addresses, specified by the recipient. In the case of faxed material, the statement shall be in at least nine-point type. In the case of e-mail, the statement shall be the first text in the body of the message and shall be of the same size as the majority of the text of the message.

30. It should be noted that in the unsolicited facsimile context, some states only require that this information be provided at the end rather than the beginning of the fax. *See id.*

31. *See, e.g.*, TENN. CODE ANN. §§ 47-18-2501(c) (1999): "Upon notification by a recipient of the recipient's request not to receive any further unsolicited faxed or e-mailed documents, no person or entity conducting business in this state shall fax or cause to be faxed, or e-mail or cause to be e-mailed, any unsolicited documents to that recipient."

for subsequent e-mail messages against the e-mail addresses of those who have previously requested to no longer receive e-mails. Failure to do so will give rise to a cause of action under many of the statutes.

Keep up to date with the spam laws. As of March 3, 2000, Congress is considering nine bills to regulate spam,[32] and twenty-five states are considering new or additional legislation addressing spam.[33] Because of the need to comply with the superset of all spam laws, it is imperative that senders of unsolicited electronic mail that wish to so comply stay current with legislative developments.

IV. DO THE SPAM LAWS WORK? SUGGESTIONS FOR LEGISLATIVE ACTION

If one assumes that state laws are a desirable and effective means of regulating spam, are the current crop of laws doing the job? If we answer in the negative, what suggestions might be advanced? One of the largest problems facing the state statutes looms on the horizon. As stated in the Introduction, the U.S. Congress is currently contemplating federal legislation governing spam. As other authors have pointed out, federal action with regard to spam is desirable.[34] However, if the Congress is wise, any legislation that is ultimately enacted will expressly preempt the state laws we have discussed. State legislators should also show foresight, as have their peers in California and Tennessee,[35] and include specific language in their legislation stating that the state laws will terminate when a federal law is enacted. If either of these two legislative actions does not occur, spam law will have the same patchwork quilt quality seen in the unsolicited fax context.[36]

States should amend their long-arm jurisdiction statutes to include out-of-state senders of spam into their borders. This will

32. S. 759 106th Cong. (1999), S. 699 106th Cong. (1999), H.R. 612 106th Cong. (1999), H.R. 1685 106th Cong. (1999), H.R. 1686 106th Cong. (1999), H.R. 1910 106th Cong. (1999), H.R. 2162 106th Cong. (1999), H.R. 3024 106th Cong. (1999), H.R. 3113 106th Cong. (1999).

33. Alaska, Arizona, California, Colorado, Connecticut, Delaware, Hawaii, Idaho, Illinois, Kansas, Kentucky, Maine, Maryland, Minnesota, Missouri, Nebraska, New Hampshire, New Jersey, New York, Oklahoma, Pennsylvania, Tennessee, Utah, Vermont and Virginia. Contact the author for citations to the various bills.

34. *See supra* note 2.

35. CA. BUS. & PROF. § 17538.4(i) (1999) and TENN. CODE ANN. §§ 47-18-2501(k) (1999), respectively.

36. Many states have laws regulating the transmission of unsolicited facsimiles. The federal government passed a law, 47 USC § 227 (1999), prohibiting unsolicited commercial facsimiles but did not preempt the state laws. This has created a complicated overlay of potential state and federal claims which depend on the state of residence of the aggrieved party.

facilitate prosecution of spammers and increase the effectiveness of the laws.

States should consider amending their small claims court statutes to allow out-of-state senders of spam to be easily served with process, and sued in small claims court. Additionally, the states should consider granting small claims courts the ability to grant injunctive relief in the case of spam prevention. Both of these small claims court statute modifications will increase the ability of recipients of spam to avail themselves of the simplest legal forum available without the complications attendant in superior or municipal courts. This in turn will enhance the deterrent effect of the laws.

Currently, it is unclear if an ISP that knowingly allows spam to be sent through its servers can be held liable under a vicarious liability theory. Since state legislatures have declared the reduction or eradication of spam desirable, their legislatures should consider the following suggestions: (1) expressly state that it will be a violation of the anti-spam law for an ISP to transmit spam with actual knowledge of such transmission, and (2) require ISPs to install spam-filtering technology within a reasonable period of time.

States need to do a more thoughtful job of defining what actually constitutes spam or "bulk" commercial e-mail.[37] Under many of the statutes, the sending of just one e-mail to just one recipient is spamming. This is probably not the intended result. The only state attempting to define "bulk" to date is Louisiana, which defines "unsolicited bulk electronic mail" as any commercial e-mail sent to more than one thousand recipients.[38] The obvious problem with this numerical definition is that many spam-facilitating programs can be used to send only 999 messages or n-1 messages, where n is the arbitrary, legislatively decreed numerical threshold defining "bulk" e-mailing or spam. While quantitative measures are probative, they should not be dispository. Legislatures should introduce a "totality of the circumstances" test that encourages a fact-finder to look at the alleged spammer's behavior in a broader context than just the number

37. The author recognizes that political economy theory contemplates purposeful ambiguity as the natural result of the inability of political actors to agree to any particular legislative definition. Because specificity may at times harm one party's vested political interest or the other or both, but faced with pressure to do *something*, legislatures have been known to pass vague laws and let the judiciary sort out the mess.

38. LA. REV. STAT. §§ 14:73.1(13) (1999). "'Unsolicited bulk electronic mail' means any electronic message which is developed and distributed in an effort to sell or lease consumer goods or services and is sent in the same or substantially similar form to more than one thousand recipients."

of e-mails sent.

Finally, even if all these suggested improvements are made, the problem of spam is not actually solved. Individuals will still get spam, particularly if a spammer only needs to comply with the consumer-protection state statutes (no misleading subject lines or spoofed headers). People will still be frustrated and angered by the dozens of spam messages they receive each day. What is needed is a broad adoption by the states, or federal enactment, of a Nevada- and California-style prohibition on unsolicited commercial e-mails that requires the senders of the spam to only send e-mail to those recipients who have expressly opted in to receiving the e-mail. The opt-in language should have teeth. For example, when a user is first registering with a site, and she is being asked if she would like to receive occasional e-mails, the default answer should be "no." Only an affirmative act of the user should constitute opt-in. Other authors have described the inherent benefits of a strong opt-in approach for consumers.[39]

V. RECENT COURT DECISIONS

State v. Heckel.[40] On March 10, 2000, King County Superior Court Judge Palmer Robinson ruled that Washington's anti-spam law is unconstitutional because "the statute in question violates the Federal Interstate Commerce Clause of the United States Constitution, [and] that the Washington statute is restrictive and burdensome. . . ." The 145-word, handwritten decision echoes a string of cases that have rejected state regulation of Internet activities. The state attorney general has decided to appeal the decision. Whether or not any state regulation of the Internet can be legal is beyond the scope of this Note.[41] However, the recent Washington decision adds urgency to the need for comprehensive, federal legislation regulating spam and preempting state law.

Fox v. Reed.[42] On March 16, 2000, the United States District Court for the Eastern District of Louisiana granted defendants' motion to dismiss a case brought by plaintiffs engaged in transmitting

39. *See generally supra* note 2.

40. State v. Heckel, Case No. 98-2-25480-7 SEA (Wa. Super. Ct. 2000).

41. For a competent lay article on the subject, *see* Carl S. Kaplan, *State Internet Laws Face a Different Constitutional Challenge*, NEW YORK TIMES ON THE WEB (visited July 2, 1999) <http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+72211+44+wAAA+July%7E2,1999%7Eand%7Einternet>.

42. Fox v. Reed, Civ. Action No. 99-3094 Section : "R"(4), 2000 U.S. Dist. LEXIS 3318 (E.D. La. Mar. 16, 2000).

bulk electronic mail. The defendants were the Attorney General of the State of Louisiana and the District Attorney for the Parish of St. Tammany. The plaintiffs facially challenged the constitutionality of the Louisiana's statute under the Fourth and Fourteenth Amendments as vague and overbroad, raised the First Amendment rights of free speech and communication, and challenged the legislation based on the Commerce Clause of the United States Constitution. Plaintiffs had not in fact been charged or threatened under the statute; rather they were seeking to have the statute declared void in anticipation of an actual act.

Ultimately, the decision of the court does not indicate whether or not the statute would survive Constitutional scrutiny. The court refused to hear the merits of plaintiffs' case. It dismissed on the basis that, because plaintiffs had not established the requirements for standing, the case did not present a justiciable case or controversy under Article III of the United States Constitution and so lacked subject matter jurisdiction.[43] The court did not address the merits of plaintiffs' assertions, leaving the door open for plaintiffs to bring their case before a court with proper jurisdiction.[44]

VI. CONCLUSION

States have leapt into the breach left by Congress' inability to agree on an approach to regulating spam on the national level. Fourteen states have already enacted spam laws. At least twenty additional states are considering their own legislation. Because of the borderless nature of the Internet and the practical problem of knowing where a recipient of spam resides, a person interested in minimizing her exposure to the anti-spam statutes must comply with the superset of these regulations. This Note analyzed the common themes or *leitmotifs* that arise in the statutes and presented suggestions for compliance with the superset of the laws. I additionally made suggestions for lawmakers to consider in crafting the new statutes to address shortcomings in the current laws.

A recent decision has declared Washington's statute unconstitutional under the dormant commerce clause, calling into question the validity of the other regulations. For a variety of reasons, this Note advocates for the prompt enactment of a federal anti-spam statute that expressly preempts the state laws and incorporates a

43. *Id.* at *27.

44. *Id.* at *6.

strong opt-in requirement. Until such a federal law is enacted, the uncertainty for plaintiffs and defendants will only increase as new states increase the roster of spam laws, complicating compliance for businesses trying to legally use spam as part of their marketing efforts.

ATMEL CORPORATION v. INFORMATION STORAGE DEVICES, INC.

Albert Smith[†] and Jennifer Ishimoto[††]

I. BACKGROUND

In June 1995, Atmel Corporation ("Atmel") sued Information Storage Devices, Inc. ("ISD") for infringement of claim 1[1] of their U.S. Patent 4,511,811 ("'811 patent").[2] The '811 patent was for a "charge pump" circuit used to boost voltage during programming operations without excessive current leakage.

In November 1995, ISD moved for summary judgment asserting that claim 1, the sole claim of the '811 patent, was indefinite under § 112, ¶ 2. Specifically, ISD alleged that the specification failed to disclose any structure corresponding to the disputed high-voltage means limitation. The specification stated only that: "[T]he present invention may include high-voltage generator circuit 34. Known

---

[†] Partner, Chairman of the Patent Subgroup of the IP Section, Fenwick & West LLP.

[††] B.S., Mechanical Engineering, University of California, Berkeley; Candidate for J.D., Santa Clara University School of Law, expected 2000.

1. This was the sole claim of the patent and read as follows:

1. An apparatus for selectively increasing the voltage on one or more of a plurality of conductive lines having inherent distributed capacitance disposed in a semiconductor circuit comprising:

means disposed on said semiconductor circuit for selecting one or more of said conductive lines; high voltage generating means disposed on said semiconductor circuit for generating high voltage from a lower voltage power supply connected to said semiconductor circuit;

voltage pulse generating means disposed on said semiconductor circuit for generating pulses;

means for capacitively coupling voltage pulses from said voltage pulse generating means to a voltage node in said semiconductor circuit;

transfer means responsive to said selecting means and connected to said voltage node for transferring increments of charge from said high voltage generating means to the inherent distributed capacitance in selected ones of said conductive lines in response to said voltage pulses;

said transfer means including switching means cooperating with said selecting means for blocking substantially all of the flow of current through and transfer of charge from said high voltage generating means to said conductive lines which are unselected.

2. Atmel Corp. v. Information Storage Devices, Inc., 198 F.3d 1374 (Fed. Cir. 1999).

Circuit techniques are used to implement high-voltage circuit 34. See On-Chip High Voltage Generation in NMOS Integrated Circuits Using an Improved Voltage Multiplier Technique, IEEE Journal of Solid State Circuits, Vol[.] SC-11, No.3, June 1976 [the "Dickson article"]."[3] The only other reference to the high-voltage generator circuit are two figures in the '811 patent that are shown as a "black box."[4] No details as to the type of electrical components that make up the circuit are given. Thus, the district court found that because no other details or description were given about the high-generator circuit within the patent, the high voltage generating means could not go beyond those described in the Dickson article.[5]

The district court then looked into whether it was permissible to incorporate by reference material not in the specification. The district court adopted the rule in the Manual of Patent Examining Procedure (MPEP), section 608.01(p), which at the time of the '811 patent application prohibited material "necessary to . . . support the claims" from being incorporated by reference to a nonpatent publication.[6] In making this ruling, the district court found that the '811 patent improperly incorporated by reference structure corresponding to the high-voltage means limitation to the Dickson article.[7] Since the specification was absent any further description of the structure limitation, the patent was found invalid as indefinite under 35 U.S.C. § 112. Thus, the district court rejected Atmel's argument that the claim should be read using the standard of "one skilled in the art," finding that one could not evade the requirements under § 112, ¶ 6 just by stating that one skilled in the art would understand it. Since previous cases had found that failure to comply with § 112, ¶ 6, violates § 112, ¶ 2 as well, the district court found that the patent was invalid on both grounds. Thus, the lower court granted summary judgment for ISD.

II. HOLDING, RATIONALE AND DISCUSSION

Atmel appealed the decision of the district court. At the heart of the appeal were two issues: (1) whether the knowledge of one skilled in the art should be considered when determining if sufficient structure is disclosed in the specification to support a means-plus-

3. *Atmel*, 198 F.3d at 1377.
4. *Id.*
5. *See id.* at 1377-78.
6. *Atmel*, 198 F.3d at 1377.
7. *See id.* at 1377-78.

function claim; and (2) whether giving the name of an article was sufficient to describe a portion of the structure supporting the means-plus-function limitation.

A. "One Skilled in the Art" Standard

The Federal Circuit first addressed the question of what is the proper standard for determining whether the structure for a means-plus-function limitation has been adequately disclosed. Section 112, ¶ 2 states that: "The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention."[8]

On appeal, Atmel argued that the district court had erred in not considering the knowledge of one skilled in the art in determining whether the high-voltage means limitation was sufficiently definite under § 112, ¶ 2, given the description in the specification.[9] ISD responded that the knowledge available to such a person cannot serve as a substitute for adequate disclosure of the structure in the specification.[10] The Federal Circuit agreed with Atmel that the knowledge of one skilled in the art should be considered.[11] "For purposes of § 112, ¶ 2, it is the disclosure in the specification itself, not the technical form of the disclosure that counts."[12]

Furthermore, the court found that the "one skilled in the art" standard applies with equal force when considering whether a means-plus-function limitation is sufficiently definite under § 112, ¶ 2.[13] To support this finding, the court cited *In re Dossel*,[14] which also involved a means-plus-function limitation. In that case, the court found that even though the word "computer" was never used in the claims or the specification, one "in the medical imaging field" would find it "well within the realm of common experience that computers are used to generate images for display by mathematically processing digital input."[15] Thus, like here, the court found that the means-plus-function limitation should not be invalid for indefiniteness.[16] Moreover, the "one skilled in the art" standard is used for most other

8. 35 U.S.C. § 112, ¶ 2 (1994).
9. *Atmel*, 198 F.3d at 1378.
10. *Id.*
11. *Id.* at 1379.
12. *Id.* at 1378.
13. *Id.* at 1379.
14. *In re* Dossel, 115 F.3d 942 (Fed. Cir. 1997).
15. *Dossel*, 115 F.3d at 947.
16. *See Atmel*, 198 F.3d at 1379.

issues relating to patents, such as claim construction, enablement, best mode, and written description.[17]

Thus, the court found that for claims involving means-plus-function limitations, the specification must adequately disclose what is meant by the claim language.[18] Failing to provide such adequate disclosure, the applicant would fail to meet the requirements of § 112, ¶ 2. However, the court found that interpreting what is disclosed must be done in light of the knowledge of one skilled in the art.[19]

B. Sufficiency of the Disclosure

The next question for the court was then whether there was sufficient disclosure of the means-plus-function limitation in the '811 patent. Atmel argued that district court erred by adopting MPEP section 608.01(p), which prohibited the incorporation of "essential material" by reference to nonpatent publications.[20] Accordingly, Atmel argued that the district court erred in holding that the structures described in the Dickson article could not be incorporated by reference into the '811 patent. Atmel contended that to find otherwise would "encourage patentees to include inordinate quantities of written material in the specification for fear of omitting 'essential material.'"[21] Alternatively, Atmel argued that the '811 patent contained sufficient structural detail just by the mention of the Dickson article.[22] Atmel relied on the testimony of an expert who stated that the mere mention of the title of the Dickson article in the specification was sufficient for one skilled in the art to envision the structure disclosed in that article.[23]

ISD, however, argued that the district court correctly followed MPEP section 608.01(p) and excluded the structures described in the Dickson article.[24] ISD argued that allowing incorporation by reference would contravene the public notice function of patents, by making it nearly impossible for the competitors to determine if they were violating a patent without burdensome reference to extrinsic evidence.[25]

17. *See id.* at 1379-80.
18. *See id.* at 1380.
19. *See id.*
20. *Id.*
21. *Id.*
22. *See Atmel*, 198 F.3d at 1380.
23. *See id.* at 1382.
24. *See id.* at 1381.
25. *Id.*

While the Federal Circuit agreed with ISD that the "means" (i.e. a structure) of a means-plus-function claim must appear in the specification, it disagreed that this determination turned on whether the patentee has "incorporated by reference" the material.[26] Instead, the court stated that the test was first whether the structure is described in the specification, and if so, whether one skilled in the art would identify the structure from that description.[27]

The court focused on the language of § 112 in rejecting the argument that other sources could not be used to define language within the claims.[28] Specifically, the court cited paragraph 6, which refers to "structure . . . described in the specification and equivalents thereof."[29] Furthermore, the court stated that "one skilled in the art," would "know[] how to makes and use a bolt, a wheel, a gear, a transistor, or a known chemical starting material. The specification would be of enormous and unnecessary length if one had to literally reinvent and describe the wheel."[30]

The court agreed with ISD that here the Dickson article may not replace a structural description in the specification, however, it found the language of the specification to be sufficient.[31] The court relied primarily on unrebutted expert testimony that the mere title of the article was "sufficient to indicate to one skilled in the art the precise structure of the means recited in the specification."[32] Thus, the court found that summary judgment finding the '811 patent invalid for indefiniteness was improper and remanded for further consideration.[33]

III. CONCLUSION/EFFECT ON PATENT LAW

In essence, the Federal Circuit held (1) that the knowledge of one skilled in the art must be considered when determining if sufficient structure is disclosed in the specification to support a means-plus-

26. *Id.*

27. *Id.* at 1381.

28. *See Atmel,* 198 F.3d at 1381-82.

29. 35 U.S.C. § 112, ¶ 6 (1994) states:

> "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support therof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."

30. *Atmel,* 198 F.3d at 1382.

31. *Id.*

32. *Id.*

33. *Id.*

function limitation; and (2) that material may be incorporated by reference from sources other than specified in the MPEP, if such material meets the standard of "one skilled in the art."

THE TORO COMPANY v. WHITE CONSOLIDATED INDUSTRIES, INC.

C. Douglass Thomas[†]

I. BACKGROUND

The Toro Company ("Toro") obtained U.S. Patent 4,694,528 ('528 patent) on September 22, 1997.[1] The '528 patent describes and claims a hand-held convertible vacuum/blower that is useful for yard work. The convertible vacuum/blower can operate in a vacuum mode or a blower mode. In the vacuum mode, the hand-held convertible vacuum/blower is able to vacuum up leaves and other debris. In the blower mode, the hand-held convertible vacuum/blower is able to blow leaves or other debris.

The primary embodiment described in the body of the '528 patent uses a restriction ring as part of an air inlet cover ("cover") to increase the pressure at an air outlet when the convertible vacuum/blower is operated in a blower mode. In other words, the restriction ring is inserted into the air inlet when in the blower mode, but removed from the air inlet when in the vacuum mode. Since the primary embodiment formed the restriction ring as part of the cover, the restriction ring was automatically inserted when the cover was in place for blower operation and was automatically removed when the cover was removed for vacuum operation. In the blower mode, the cover is attached to the housing of the convertible vacuum/blower using a tab and detent system.

White Consolidated Industries, Inc. and WCI Outdoor Products, Inc. (together "White") manufactured and sold a competing convertible vacuum/blower. White's product had a cover and a restriction ring for an air inlet, but the restriction ring was a separate part from the cover. To operate White's product as a blower, the

---

[†] Mr. Thomas is a partner in the Silicon Valley office of Beyer Weaver & Thomas, LLP. This case note reflects the present thoughts of the author, which should not be attributed to Beyer Weaver & Thomas, LLP or any former, current or future clients of Beyer Weaver & Thomas, LLP. The author is grateful for the assistance provided by Mr. David Banie for his help in preparing this case note.

1. U.S. Pat. No. 4,694,528 to Comer et al. ("528 patent").

restriction ring had to be manually inserted into an air inlet opening and then covered by the cover. To operate as a vacuum, the cover would be opened and the restriction ring manually removed from the air inlet opening. Further, with White's product, the cover was attached to the housing by a hinge and latch mechanism.

Toro sued White in the U.S. District Court for the District of Minnesota for infringement of claims 16 and 17 of the '528 patent.[2] The district court granted Toro's Motion for Summary Judgement that claim 16 of the '528 patent was literally infringed by White's product.[3] The district court, however, did not consider infringement under the doctrine of equivalents. White then appealed the district court's decision to the U.S. Court of Appeals for the Federal Circuit ("Federal Circuit").

II. FEDERAL CIRCUIT'S DECISION AND ANALYSIS

This case turned on claim construction. As expected, the Federal Circuit construed claim 16 *de novo* because claim construction is a question of law. Even so, the panel, consisting of Judges Newman, Friedman and Rader, did not all agree. Judges Newman and Friedman signed on to a majority opinion, while Judge Rader authored a dissenting opinion. The majority's opinion is discussed below, followed by a brief discussion of the dissenting opinion.

The claim at issue, claim 16, was as follows:

> 16. A convertible vacuum-blower comprising:
>
> [1] a housing having an air inlet and an air outlet;
>
> [2] a motor supported in said housing
>
> [3] an impeller having a plurality of impeller blades supported for rotary motion in said housing, in fluid communication with said air inlet and said air outlet, and rotatably driven by said motor;
>
> [4]a removable air inlet cover for covering said air inlet, said air inlet cover having apertures for passage of air through the cover;
>
> [5]attachment means for removably securing said air inlet cover to said housing; and

---

2. Toro Co. v. White Consolidated Indus., Inc., 199 F.3d 1295 (Fed. Cir. 1999).

3. *See* Toro Co. v. White Consolidated Indus., Inc., 920 F. Supp. 1008, 1019 (D. Minn. 1996). Toro had conceded to the district court that claim 17 was not literally infringed. *See Toro*, 199 F.3d at 1298.

> [6]said cover including means for increasing the pressure developed by said vacuum-blower during operation as a blower when air is being supplied to said impeller through said apertured cover.[4]

On appeal, Toro and White disputed the interpretation of two particular phrases within claim 16. Specifically, the phrases of claim 16 in dispute were: (1) "attachment means for removably securing said air inlet cover to said housing" (clause 5), and (2) "cover including means for increasing the pressure" (clause 6).

With respect to the law of claim construction, the majority wanted to interpret the claim as would a person of experience in the field.[5] Although the words in dispute were ordinary or common, the majority felt that the dictionary definitions proffered by each side were not particular helpful.[6] The majority summarized their notion of claim construction as follows:

> In judicial "claim construction" the court must achieve the same understanding of the patent, as the document whose meaning and scope have legal consequences, as would a person experienced in the technology of the invention. Such a person would not rely solely on a dictionary of general linguistic usage, but would understand the claims in light of the specification and the prior art, guided by the prosecution history and experience in the technologic field.[7]

A. First Disputed Claim Phrase: Attachment Means

The first claim construction issue concerned the claim element "attachment means for removably securing said air inlet cover to said housing" of clause 5 in claim 16. There was apparently no dispute over whether this claim limitation should be interpreted according to

---

4. *Toro*, 199 F.3d at 1298. Claim 16, '528 patent (bracketed numerals added by court). It is interesting to note that the '528 patent had 17 claims, of which only claims 1 and 16 were independent claims. *See* '528 patent at col. 7-10. Claim 1, although generally similar to claim 16, was not asserted. Claim 1 is directed to a convertible vacuum/blower but its novelty is focused on a safety switch mechanism that allowed the motor to operate when the air inlet was covered but not when the air inlet was uncovered. *See id.* at col. 7 (lines 30-47). Claim 16, in contrast, did not include any safety switch mechanism limitations, as its novelty was focused on the "including" of means for increasing the pressure during operation as a blower. *See id.* at col. 9 (lines 14- 18) to col. 10 (lines 1- 11)..

5. *See Toro*, 199 F.3d at 1299.

6. *See id.*

7. *Id.*

35 U.S.C. § 112, ¶ 6 which is means plus function claim style.[8] The '528 patent described the invention as using a tab and detent system to secure an air inlet cover to the housing of the convertible vacuum/blower. As a result, the tab and detent approach of the '528 patent rendered the air inlet cover completely removable from the housing. In contrast, the White's product used a hinged cover instead of a tab and detent design. As a consequence, White's cover was not completely removable because it always remained attached at the hinge.[9] The majority agreed with the district court that the phrase "removably securing" does not require that the cover be entirely separate from the housing, but instead merely refers to removal of the cover from the air inlet.[10]

The majority then concluded that the district court did not clearly err in ruling that the hinge and latch of White's product were equivalent the tab and detent approach described in the '528 patent.[11] To support this conclusion, the majority points to interchangeability as evidenced by a prior art reference.[12] Specifically, the majority stated: "[t]he use of a latch with a hinged cover is shown in the prior art, performing the identical function of securing the cover to the air inlet during use as a blower, using known interchangeable structures."[13] Despite the design differences, the majority found the attachment means present in White's product. Thus, the majority affirmed the district court's interpretation of the first disputed claim phrase (clause 5).

B. Second Disputed Claim Phrase : Including

The other claim construction question concerned whether clause 6 in claim 16 covers a restriction ring that is not attached to the cover. The pertinent claim language of clause 6 is "said cover including means for increasing the pressure. . . ." Recall, the description of the

---

8. *See* 35 U.S.C. §112 ¶ 6 (1994).

9. *See Toro*, 199 F.3d at 1299. (White unsuccessfully argued that the '528 patent did not intend to include an attached cover.) The prior art reference was apparently U.S. Pat. No. 4,325,163 to Mattson et al. which is not only mentioned in the background section of '528 patent but also a cited reference on the '528 patent's front page. *See* '528 patent at front page and col. 1 (lines 10- 38).

10. *See Toro*, 199 F.3d at 1300.

11. *See id.* Note the "clear error" standard of review applied to the equivalence determination under 35 U.S.C. § 112, ¶ 6 (1994).

12. *See id.* It is interesting to note here that the scope of equivalents provided to the attachment means seems to be relatively large given that the hinge and latch design was found to be equivalent to the tab and detent design.

13. *Id.*

primary embodiment of the invention in the '528 patent is a restriction ring as part of the air inlet cover, whereas in White's product, the restriction ring is a separate part from the cover. In the '528 patent, the restriction ring is the structure responsible for the means for increasing pressure.

The district court found that: "the term 'including,' correctly construed, 'suggests the containment of something as a component or subordinate part of a larger whole,' and comprehends a separate restriction ring that is not part of the cover but is separately inserted and removed."[14] In other words, the district court concluded that the cover includes the restriction ring regardless of whether attached to the cover.

On review, the majority noted that this claim construction question—as to whether the restriction ring must be attached to the cover—was not a question under 35 U.S.C. § 112, ¶ 6. The majority considered various things in interpreting whether the words "including" and "cover", as a matter of law, require that the cover and the ring be attached to each other. The majority noted that "[t]he specification and drawings show the restriction ring as 'part of' and permanently attached to the [air inlet] cover."[15] It is also true, as the majority noted, that the specification of the '528 patent does not state that the flow restriction ring and the air inlet cover can be two distinct components.[16] The majority then goes on to disparage the specification of the '528 patent. Specifically, the majority opinion states:

> The specification shows only a structure whereby the restriction ring is "part of" the cover, in permanent attachment. This is not simply the preferred embodiment; it is the only embodiment. . . . The description of the invention states that the ring is inserted and removed "automatically" when the cover is inserted or removed. Thus when the cover is closed for operation in the blower mode, the ring that is "attached to the inside of the air inlet cover by a plurality of screws" is thereby put into place. It is inserted simply

14. *Id.* (citation omitted).

15. *Id.* at 1301. This is correct. FIG. 4 of the '528 patent shows a ring 76 formed with an insert 72 that is attached to an air inlet cover 50 (col. 4, lines 47-53; col. 5, lines 19-22). Further, at column 7, lines 6-7 the specification refers to the flow restriction ring 76 as part of the air inlet cover 50. Hence, it is clear that the preferred embodiment of the invention described in the '528 patent formed the flow restriction ring (i.e., means for increasing pressure) as attached or part of the air inlet cover. *See* '528 patent.

16. *See Toro*, 199 F.3d at 1301.

by closing the cover; it is removed by opening the cover.[17]

Finally, the majority concluded that "[t]he specification does not describe an invention broader than this description of the cover and the restriction ring 'automatically' inserted and removed together."[18] In anticipation of the dissent's objections, the majority also states: "[t]his is not a case of limiting the claims to a 'preferred embodiment' of an invention that has been more broadly disclosed. It is well established that the preferred embodiment does not limit broader claims that are supported by the written description."[19]

Toro also attempted to broaden the interpretation of "including" by relying on the doctrine of claim differentiation. Claim 17 depends from claim 16 and, among other things, indicates that the restriction ring is "carried by the cover." Hence, claim 17 would seem to support (under the guise of the doctrine of claim differentiation) requiring that the term "including" be broadly read as Toro desired. Instead, the majority concluded that "the doctrine of claim differentiation does not serve to broaden claims beyond their meaning in light of the specification, . . . and does not override clear statements of scope in the specification and prosecution history."[20]

Accordingly, the majority found that the term "including" of clause 6 in claim 16 required that the restriction ring be attached to the cover. Thus, the majority reversed the district court's interpretation of clause 6 in claim 16.

III. DISSENTING OPINION

The dissenting opinion by Judge Rader finds at least three areas where he believed the majority's opinion was wrong in narrowly construing the term "including." First, ordinary dictionaries and law dictionaries leave no doubt that the ordinary meaning of "includes" is not limited to physical attachment.[21] Second, traditionally speaking, the term "including" is used to signify a broader relationship than

17. *Id.*

18. *Id.* Note that the Federal Circuit cites 37 C.F.R. § 1.83(a) (1999) ("The drawing in a nonprovisional application must show every feature of the invention specified in the claims.") as somehow supporting their position, unfortunately, 37 C.F.R. 1.83(a) has nothing to do with claim construction.

19. *Toro*, 199 F.3d at 1301. (citing, e.g., Laitram Corp. v. Cambridge Wire Cloth Co., 863 F.2d 855, 865 (Fed. Cir. 1988)). Question: Was claim 16 part of the original description that could bootstrap itself as self-defining the scope of the invention and therefore never be broader than that disclosed?

20. *Id.* at 1302 (citations omitted).

21. *See id.* at 1303 (Rader, J., dissenting).

merely being attached.[22] Third, Judge Raider believed that the specification described more than one embodiment, specifically, an embodiment in which the flow restriction ring is not permanently attached to the cover.[23]

IV. CONCLUSIONS

As to the first disputed claim phrase, the Federal Circuit allowed the prior art to expand claim coverage with respect to equivalents for means plus function elements. Although this result was assisted somewhat by the clearly erroneous standard of review, it is nevertheless significant that prior art was used to broaden the available range of equivalents. While means plus function claim elements are not generally restricted by the prior art, courts have been reluctant to provide such claim elements anything but a narrow scope of equivalents. Here, the background section of the '528 patent mentioned the prior art reference that assisted with broadened equivalents determination, but its discussion of the prior art reference was with respect to a general introduction of convertible vacuum/blowers and thus was not in reference to a particular problem that the invention solved.[24]

As to the second disputed claim phase, the majority's narrow reading of the term "including" resembles the Federal Circuit's trend in interpreting claims narrowly when there is doubt as to what is covered. However, in this case, the meaning of the term "including" was sufficiently clear and there was no reasonable justification for the majority's narrow interpretation.

The majority's failure to appreciate the specification led them to erroneously conclude that the specification had clear statements against the ring being anything but attached to the cover. Unlike the majority's conclusions, there are no clear statements of scope in the specification or the prosecution history that would lead someone to believe that "includes" should be narrowly read.[25] Further, looking at

---

22. *See id.*

23. *See id.* at 1303-1304. Here, the dissenting opinion states: "More important, the inventor contrasts the preferred embodiment not, as the court thinks, with disadvantageous prior art, but rather with a less-preferred embodiment of the invention at hand: a blower with a replaceable, i.e., non-attached, ring." *Id.* at 1303. *See also* '528 patent, col. 7 (lines 6-12).

24. The problems associated with the prior art were however not focused on the attaching of the cover, but instead on safety hazards when converting its modes as well as on velocity of air being output.

25. The majority points to nothing in the prosecution history as assisting their interpretation.

the language at column 7, lines 6-12 of the '528 patent (on which the majority places so much emphasis), one should note that it states that the automatic nature of removing of the ring (by being part of the cover) is "also advantageous." The word "also" suggests that this feature of the invention is not mandatory. In other words, this section of the '528 patent is indicating that it is advantageous to have the restriction ring part of the cover. Normally, such a statement would suggest that the feature is then an optional (i.e., not mandatory) feature of the invention. The majority's reading of this same portion of the '528 patent to say that there are clear statements of scope in the specification for their narrow interpretation is without justification. The dissent is much closer to the mark on this point.

The majority has narrowed the term "including" to the primary embodiment described in the '528 patent. However, patent practitioners, those who actually write the patent claims, would not have construed the term "including" the way that the majority opinion does. The term "including" is designed to be a broad open-ended term.[26] It is not intended to provide a structural indication in most cases. According to the majority's rationale, the interpretation of the term "including" was read in a narrow fashion because the majority felt that was the scope that was described in the body of the specification.[27]

Still further, dependant claim 17 with the help of the doctrine of claim differentiation clearly indicates that "including" in claim 16 was intended to be broader than "carried by" as was used in claim 17. The majority shows no respect for the beleaguered doctrine of claim differentiation. Had the majority had any respect for the doctrine, this case would have seemed to be the perfect situation where the doctrine would be helpful in determining whether the applicant intended to use

---

26. It is also used essentially interchangeably with "comprising," particularly when used as a transition phrase. *See, e.g.*, J. LANDIS, MECHANICS OF PATENT CLAIM DRAFTING § 7 (1970); DONALD S. CHISUM, CHISUM ON PATENTS § 8.06[1][b], at 8-101 (1998) ("including" can also be used to draft an "open" claim); Hewlett Packard Company v. Repeat-O-Type Stencil Manufacturing, 123 F.3d 1445, 1451 (Fed. Cir. 1997) (claim term "including" is synonymous with "comprising" as a transition phrase at least thereby permitting the inclusion of unnamed components).

27. While the body of the specification was such that the primary embodiment did have the ring attached to the cover, if a patent practitioner had intended the claims to be so limited, they would have used language such as "part of" or "attached" in the claim instead of "including". The majority also ignores column 7, lines 12-18 of the '528 patent which states that another advantage of the invention is using a safety switch mechanism. This advantage was not mandatory to claim 16, but the majority's improper reading of the preceding sentence in the '528 patent was deemed mandatory. In reality, these were merely recitations of potential advantages obtained by the invention, not mandatory requirements.

the term "including" broadly.

In effect, the majority's opinion suggests that regardless of what language a claim may use, the claim can be limited to the primary embodiment described in the body of the patent's specification. In other words, the majority suggests that claims cannot be construed apart from the specification and that claims, which are potentially broader, can be narrowly construed. This suggestion of the majority's opinion is wrong because the claims define the invention and can exceed the scope of the body of the specification. Of course, one could always blame the patent practitioner for perhaps not using the best choice of claim language for clause 6 in claim 16.[28]

Another interesting result of this case was that the first disputed claim phrase, which was interpreted under 35 U.S.C. § 112, ¶ 6, was given a liberal interpretation, while the second disputed claim phrase, which was not interpreted under 35 U.S.C. § 112, ¶ 6, was given a restrictive interpretation. In any event, the case was remanded back to the district court for consideration of whether White's product infringes claim 16 under the doctrine of equivalents. If the prior art and the prosecution history allow, White's product would likely be found to infringe claim 16 under the doctrine of equivalents.

28. Namely, claim 16 would have been better if the means for increasing the pressure were recited simply as that and not utilizing the associative language "said cover including."

GEOFFREY H. PALMER v. TRUCK INSURANCE EXCHANGE: AN ANALYSIS OF INSURANCE COVERAGE FOR TRADEMARK INFRINGEMENT

Michael Traynor[†] and Alison Choppelas[††]

I. INTRODUCTION

This action for insurance coverage arose out of the settlement of an underlying action for trademark infringement.[1] The California Supreme Court considered whether certain insurance policy provisions relating to advertising liability arising from "title" or "slogan" infringement covered infringement of a trademarked name. The court, interpreting the provisions narrowly, held that the policy provisions at issue did not provide coverage for the infringement of a trademark. As interpreted by the court, the coverage clause only insured against infringement of names of literary or artistic works or names that were slogans. The clause did not insure against infringement of a trademarked word embodied in a slogan. Further, the court found that an exclusion clause in the policy expressly excluded coverage for infringement of a registered trade mark, service mark or trade name unless that trade mark, service mark or trade name was a title or slogan. The court analyzed the meaning of the word "title" and found that "title" could not subsume the definitions of "trademark," "service mark," or "trade name" as understood in the policy. The only meaning of the word "title" that fit within the interpretation of the policy was that embodied in the name of a literary or artistic work. Having found that the policy did not cover trademark infringement, the court did not reach the second issue of whether Insurance Code section 533 would bar indemnity for willful trademark infringement.

[†] Partner, Cooley Godward LLP, San Francisco, California. J.D., Harvard Law School, 1960.

[††] Candidate for J.D., Santa Clara University School of Law, 2000. The authors would like to thank the editors of the Santa Clara Computer and High Technology Law Journal for their efforts.

1. *See generally* Palmer v. Truck Ins. Exch., 21 Cal. 4th 1109, 988 P.2d 568, 90 Cal. Rptr. 2d 647 (1999).

II. FACTUAL AND PROCEDURAL BACKGROUND

This case arose from a dispute over trademark infringement of a registered mark used to identify a real estate developer in Santa Clarita Valley. Newhall Land and Farming Company ("Newhall") sued Easton Investments II ("Easton") and Westcreek Properties, Ltd. ("Westcreek"), for infringement of the registered mark "Valencia" ("Newhall action").[2] Geoffrey H. Palmer, appellee in this action, was the general partner of both Easton and Westcreek. A jury found that Easton and Westcreek had infringed Newhall's trademark, and awarded Newhall damages of nearly $2.3 million.[3] The jury also found that Newhall and Westcreek's conduct was "willful."[4] Easton and Westcreek appealed from the trial court's judgment entered on the jury's verdict.

Soon after the jury verdict, Palmer tendered the Newhall action to various insurance carriers, including Truck Insurance Exchange ("Truck"), the defendant in this action. Truck agreed to pay a portion of the fees and costs of the appeal but reserved the right to contest coverage of any infringement found against Easton and Westcreek. During the pendency of the appeal, the Palmer defendants settled the case with Newhall for $1,590,000.[5] Truck denied coverage and refused to contribute to the settlement.

The comprehensive umbrella liability policy ("Policy"), issued by Truck to Palmer, is the policy at issue in this appeal.[6] The Policy provided coverage for "advertising liability," defined as: "(1) Libel, slander or defamation; . . . (2) Infringement of copyright or of title or of slogan; . . . committed or alleged to have been committed in any advertisement, publicity article, broadcast or telecast and arising out of the named insured's advertising activities."[7] The Policy excluded coverage for trademark infringement:

> This insurance does not apply, . . . with respect to advertising activities, to claim[s] made against the insured for . . . infringement of registered trade mark, service mark or trade name by use thereof

---

2. *See id.* at 1112, 988 P.2d at 571, 90 Cal. Rptr. 2d at 650.

3. *See id.*

4. *See id.*

5. *See id.* at 1113, 988 P.2d at 571, 90 Cal. Rptr. 2d at 651.

6. The preliminary policies issued by the various insurance carriers were not at issue before the California Supreme Court. The Court of Appeals concluded that the Plaintiffs were not named insureds on the preliminary policies. The parties did not contest this part of the Court of Appeal's ruling.

7. *See Palmer*, 21 Cal. 4th at 1114, 988 P.2d at 571, 90 Cal. Rptr. 2d at 651 (describing the terms of the Policy in question).

> as the registered trade mark, service mark or trade name of goods or services sold, offered for sale or advertised, but this shall not relate to titles or slogans . . .[8]

Palmer, Easton, and Westcreek, among others, sued Truck, and other insurers not party to this appeal, seeking declaratory relief and alleging a breach of the implied covenant of good faith and fair dealing and a breach of the duty to defend.[9] Truck demurred. With respect to the complaint, Truck argued that the "no action" clauses in each of its policies foreclosed the plaintiffs' lawsuit because plaintiffs settled the Newhall action without Truck's authorization. Truck also argued that the policies excluded coverage for trademark infringement. It further asserted that there was no duty to defend or indemnify plaintiffs because the Newhall jury found the plaintiffs' conduct willful. Finally, Truck argued that plaintiffs were not insured under the Truck policies because they were not named in the policies and thus lacked standing to sue.[10] The trial court sustained Truck's demurrer without leave to amend on grounds that the Palmer defendants lacked standing to sue and breached the "no action" clauses of their policies. Consequently, the court dismissed Truck from the case.[11] The plaintiffs appealed.

The Court of Appeal reversed the trial court, holding that the plaintiffs did have standing and did not breach the "no action" clause of the Policy. The court also held that the defendant's conduct was not willful within the meaning of Insurance Code section 533[12] and that the terms "title" or "slogan" were not limited to artistic or literary works for the purposes of covering infringement.[13]

Truck sought review in the California Supreme Court, which granted review to consider two questions: (1) whether policy language providing coverage for advertising liability caused by infringement of title or of slogan, but excluding coverage for infringement of trade mark, service mark or trade name (except relating to) titles or slogans, covers infringement of any name; and (2) whether Insurance Code section 533 bars indemnity for willful

8. *Id.*

9. *See id.* at 1113, 988 P.2d at 571, 90 Cal. Rptr. 2d at 651.

10. *See id.*

11. *See id.*

12 Palmer v. Truck Ins. Exch., 78 Cal. Rptr. 2d 389, 402 (Ct. App. 1998) (previously published at 66 Cal. App. 4th 916). This case has been ordered depublished pending review by the California Supreme Court.

13. *See id.* at 407.

trademark infringement.[14]

III. DISCUSSION

The parties agreed that Truck had no duty to reimburse the plaintiffs for the settlement during the pendency of the Newhall appeal if the California Supreme Court found that the Policy did not cover the underlying district court judgment.[15] The dispositive issue, therefore, was whether the policy language relating to advertising liability actually covered a judgment based on infringement of a name like "Valencia."[16] The analysis centered on the interpretation of the policy definition of "advertising liability," which included "Infringement of copyright or of title or of slogan."[17] The Court of Appeal and the Supreme Court disagreed on the interpretation of the words "title" and "slogan." The Supreme Court overruled the Court of Appeal, concluding that the infringement of the trademark "Valencia" was not covered by the terms "title" and "slogan."[18]

Both courts analyzed various meanings of the word "title" based on many dictionary definitions of the word. While the Court of Appeal relied on a broad definition incorporating the "ordinary and popular sense" of the term "title,"[19] the Supreme Court narrowed the interpretation of "title" to the specific use of the term in the Policy.[20] The Supreme Court concluded that, in the context of the coverage clause, "title" could only mean the name of a literary or artistic

14. *See Palmer*, 21 Cal. 4th at 1114, 988 P.2d at 572, 90 Cal. Rptr. 2d at 652. California Insurance Code section 533 provides: "An insurer is not liable for a loss caused by the wilful act of the insured; but he is not exonerated by the negligence of the insured, or of the insured's agents or others." CAL. INS. CODE ANN. § 533 (WEST 1999).

15. *See Palmer*, 21 Cal. 4th at 1114, 988 P.2d at 572, 90 Cal. Rptr. 2d at 652.

16. *See id.*

17. *Id.* at 1114, 988 P.2d at 571, 90 Cal. Rptr. 2d at 651.

18. *See id.* at 1119, 988 P.2d at 575, 90 Cal. Rptr. 2d at 655.

19. *See Palmer*, 78 Cal. Rptr. 2d at 405. The Court of Appeal relied on the following definitions of the word "title:" "A mark, style, or designation; a distinctive appellation; the name by which anything is known." BLACK'S LAW DICTIONARY 1331 (5th ed. 1979); and "1. the name of a book, chapter, poem, essay, picture, statue, piece of music, play, movie, etc.... 3. a descriptive name or appellation; epithet." WEBSTER'S NEW WORLD DICTIONARY 1492 (2d college ed. 1980). "Epithet" in turn, is defined as "1. an adjective, noun, or phrase used to characterize some person or thing,... 2. a descriptive name or title." *Id.* at 472. "Appellation" is defined as "1. the act of calling by a name, 2. A name or title that describes or identifies a person or thing; designation." *Id.* at 66. Similarly, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 2400 (Ed. 1993) gives fourteen definitions for "title," including: "7. a descriptive name, a distinctive appellation or designation..."

20. *Palmer*, 78 Cal. Rptr. 2d at 405.

work.[21]

The Court of Appeal interpreted the phrase "Infringement of copyright *or* of title or of slogan," (emphasis added) as used in the policy's definition of "advertising liability" to separate the concepts of "copyright" from "title" or "slogan." It reasoned that the express exclusion for trademark infringement in the exclusion clause contemplates that there may be an infringement of title or slogan without reference to copyright.[22] The Court of Appeal analogized the case to *A Touch of Class Imports, Ltd. v. Aetna Casualty and Surety Co.*[23] In *A Touch of Class*, the court concluded that a trademarked phrase used within a title or slogan was covered by the definition of advertising liability.[24] In the Newhall action, the appellees were charged with using the mark "Valencia" in conjunction with the name of various building developments.[25] Without elaboration, the Court of Appeal concluded that using the mark in the development titles fell within the terms of the Policy and the Policy did not limit coverage to copyrightable artistic or literary work.[26] The Court of Appeal decided that the Policy's use of the terms "title" and "slogan" was broad enough to encompass use of the "Valencia"[27] mark. The use of "Valencia" therefore constituted an infringement.

The Supreme Court, however, disagreed with the Court of Appeal's findings. The court noted that "title" appears in both the coverage clause defining advertising liability and the trademark exclusion clause. There was no evidence within the Policy suggesting that the use of "title" changed from clause to clause.[28] Thus, the court assumed that "title" had the same meaning in each clause of the Policy. The exclusion clause stated that

> [t]his insurance does not apply . . . with respect to advertising activities, to claim[s] made against the insured for . . . infringement of registered trade mark, service mark, or trade name by use thereof as the registered trade mark, service mark or trade name of goods or services sold, offered for sale or advertised, but this shall not relate to titles or slogans . . .[29]

---

21. *See id.*
22. *See id.*
23. 901 F. Supp. 175 (S.D.N.Y. 1995).
24. *See id.* at 176.
25. *See Palmer*, 21 Cal. 4th at 1112, 988 P.2d at 571, 90 Cal. Rptr. 2d at 650.
26. *See Palmer*, 78 Cal. Rptr. 2d at 407.
27. *See id.*
28. *See Palmer*, 21 Cal. 4th at 1116, 988 P.2d at 573, 90 Cal. Rptr. 2d at 653.
29. *Id.* at 1117, 988 P.2d at 573-74, 90 Cal. Rptr. 2d at 653.

The court interpreted this clause to exclude coverage for infringement of a "registered trade mark, service mark or trade name" unless that "trade mark, service mark or trade name" was a title or slogan. Thus, if the definition of "title" subsumed the definitions of "trade mark," "service mark," or "trade name" as understood in the Policy, the rest of the exclusion clause would be rendered meaningless.[30] The court concluded that the word "title" in the Policy referred only to the name of a literary or artistic work.[31] Because the infringed mark "Valencia" was not the name of a literary or artistic work, the Policy provision providing coverage for infringement of titles did not apply and Truck was not required to reimburse the plaintiffs' settlement.[32]

The Supreme Court also found that the word "slogan" did not apply to the present action.[33] The court relied on the Court of Appeal's holding in another case, which stated: "While an insurer has a duty to defend suits which potentially seek covered damages, it has a duty to indemnify only where a judgment has been entered on a theory which is actually (not potentially) covered by the policy."[34] In the Newhall action, the jury found that the plaintiffs infringed Newhall's trademark, not its slogans. The jury awarded damages on profits realized from the infringing use of Newhall's mark, not from the use of its slogans. Thus, the Supreme Court reasoned that the Newhall judgment was entered on the theory of the plaintiffs' infringement of mark, not the infringement of any slogans.[35] The Court stated that although Newhall may have used the mark in a slogan, this did not bring the judgment within the scope of coverage for infringement of that slogan. Relying on the definition of a slogan as "a brief attention-getting phrase used in advertising or promotion" or a "phrase used repeatedly, as in promotion,"[36] the court concluded that "infringing use of a trademark that is merely a word in a phrase used as a slogan is not the same as the infringing use of a slogan."[37]

---

30. *See id.* at 1117, 988 P.2d at 574, 90 Cal. Rptr. 2d at 653-54.

31. *See id.* at 1119, 988 P.2d at 575, 90 Cal. Rptr. 2d at 655.

32. *See id.* at 1119, 988 P.2d at 575, 90 Cal. Rptr. 2d at 655-66.

33. *See id.* at 1120, 988 P.2d at 576, 90 Cal. Rptr. 2d at 656.

34. *Palmer*, 21 Cal. 4th at 1120, 988 P.2d at 576, 90 Cal. Rptr. 2d at 656 (quoting Collin v. Am. Empire Ins. Co., 21 Cal. App. 4th 787, 802, 26 Cal. Rptr. 2d 391, 398 (Ca. Ct. App. 1994)).

35. *See id.*

36. *Id.* (quoting WEBSTER'S COLLEGIATE DICTIONARY (10th ed. 1993) and AM. HERITAGE COLLEGE DICT. (3d ed. 1993), respectively).

37. *Id.*

Therefore the plaintiffs' infringement of the "Valencia" mark was not covered by the word "slogan" as defined in the Policy.

IV. INSURANCE CODE SECTION 533

Having held that the Policy did not insure against the plaintiffs' infringement, the California Supreme Court did not reach the question of whether Insurance Code section 533 bars indemnity for willful trademark infringement. Since the question was resolved by the Court of Appeal, however, it warrants a brief discussion here.

In its argument to the Court of Appeal, Truck relied on Insurance Code section 533, contending that public policy precluded insurance coverage for willful acts of infringement. The lower court disagreed, citing *J.C. Penney Casualty Ins. Co. v. M.K*[38] and *Clemmer v. Hartford Insurance Co.*[39] These cases limited the meaning of "willful" in section 533 to circumstances in which an act is inherently harmful or committed with a "preconceived design to inflict harm."

An analogous Ninth Circuit case, *Zurich Ins. Co. v. Killer Music, Inc.*,[40] cited these same cases. In *Zurich*, the Ninth Circuit reversed a summary judgment order in favor of an insurer on the ground that the actions of the insured were not proven willful in the underlying copyright suit within the meaning of section 533. The *Zurich* Court reasoned:

> A "clear line of authority" in California directs that "even an act which is 'intentional' or 'willful' within the meaning of traditional tort principles will not exonerate the insurer from liability under [§] 533 unless it is done with a 'preconceived design to inflict injury'" (citations omitted). The term "willful" is used to describe "an act done with malevolence," (citation omitted), or with "malice in fact" (citation omitted). A "'willful act' within the meaning of section 533 means 'something more than the mere intentional doing of an act constituting [ordinary] negligence,' and appears to be something more than the intentional violation of a statute" (citation omitted) (brackets in original).[41]

Although subjective harm need not be proven and can be assumed from the facts, copyright infringement is not an act that is willful per se.[42] In *Palmer*, the Court of Appeal held that trademark

38. 52 Cal. 3d 1009, 804 P.2d 689, 151 Cal. Rptr. 64 (1991).

39. 22 Cal. 3d 865, 587 P.2d 1098, 151 Cal. Rptr. 285 (Ca. Sup. Ct. 1978).

40. 998 F.2d 674 (9th Cir. 1993).

41. *Id.* at 678.

42. *See id.* at 674.

infringement is also an act that is not willful per se, and that the plaintiffs' infringement did not satisfy either of the definitions of willfulness discussed above.[43] The court pointed out that wrongful intent is not an element of trademark infringement; it is merely a factor the court may consider in deciding whether to award enhanced damages and attorney's fees.[44] Since the court in the Newhall action decided against awarding enhanced damages and attorney's fees, even though the jury found Easton and Westcreek's infringement to be willful, the Appellate Court in the Truck dispute refused to find that the conduct was willful as a matter of law.

V. OTHER RELATED CASES

In *Gulf Ins. Co v. Contreras*,[45] the Ninth Circuit U.S. Court of Appeals appeared to have reached a different result than the *Palmer* court on res judicata grounds. Affirming the District Court, the Ninth Circuit ruled that Aetna Casualty & Surety Co. had a duty to defend its insureds in a trademark dispute.[46] Aetna had litigated its duty to defend in the state court and lost. The District Court, affirming that decision, gave full faith and credit to the state court's decision.[47] The Ninth Circuit stated that the District Court properly invoked the doctrine of res judicata and collateral estoppel to preclude Aetna from raising the issue of whether it owed a duty to defend the insureds in the state court litigation.[48]

In *Mez Industries, Inc. v. Pacific National Insurance Company*,[49] a case seeking insurance coverage against a patent infringement claim, the Court of Appeal reached a different result from the *Palmer* court on the Insurance Code section 533 issue. In *Mez Industries*, a liability insurer providing coverage for an advertising injury refused to defend its insured against an action charging the insured with inducement of patent infringement.[50] The plaintiff alleged that the insured, a component manufacturer, used its advertising to encourage its customers to put the components together in a way that infringed

43. *See Palmer*, 78 Cal. Rptr. 2d at 402.

44. *See id.* at 401.

45. No. cv-95-2260, 1999 WL 1040120 (9th Cir., Nov. 16, 1999).

46. *See id.* at *1.

47. *See id.*

48. *See id.* In reaching that conclusion, the Ninth Circuit declined to decide whether a state court's judgment on an insurer's duty to defend constitutes a final judgment or an interlocutory order under California law.

49. 76 Cal. App. 4th 856, 90 Cal. Rptr. 2d 721 (Ct. App. 1999).

50. *See id.* at 861-62, 90 Cal. Rptr. 2d at 724.

the plaintiff's patents.[51] The insurance policy provided for indemnity and defense for injury caused by misappropriation of advertising ideas or style of doing business and for infringement of copyright, title, or slogan in the course of advertising. In the insured's ensuing action for declaratory relief and breach of contract against the insurer, the trial court sustained the insurer's demurrer without leave to amend and entered a judgment of dismissal.[52] The Court of Appeal affirmed, holding that no duty to defend ever arose, since the advertising injury provisions of the policy did not provide coverage to the insured for inducement of patent infringement.[53] The court applied common sense to the context of this case, stating that the policy terms could not reasonably be read to include either patent infringement or the inducement thereof.[54] Moreover, even if the policy language was not totally free from ambiguity, the insured could not have had an objectively reasonable expectation of coverage for a claim of inducing willful patent infringement.[55] The court also held that coverage would have been precluded by Insurance Code section 533, since an inducement to patent infringement cannot be committed except as a knowing, intentional, and purposeful act that is clearly wrongful and necessarily harmful.[56] Appellate review to the California Supreme Court was denied March 22, 2000.

VI. CONCLUSION

After analyzing the policy provisions, the California Supreme Court in *Palmer* concluded that appellee's trademark infringement of "Valencia" was not covered within the meaning of "title" or "slogan," and therefore appellant was exonerated from having to pay appellee's settlement in the Newhall action. However, had the court concluded in favor of appellee, it is unclear how the court would have resolved the Insurance Code section 533 issue. Reconciling *Mez Industries* with *J.C. Penney*, *Clemmer*, and *Zurich*, it appears that the Court of Appeal's resolution of the issue turns on whether one of the elements of infringement of the intellectual property at issue includes willful intent. Since a finding of trademark infringement does not require a finding of willfulness and infringement of a patent does, the Court of

51. *See id.* at 863, 90 Cal. Rptr. 2d at 725.
52. *See id.* at 864, 90 Cal. Rptr. 2d at 726-27.
53. *See id.* at 875, 90 Cal. Rptr. 2d at 734.
54. *See id.*
55. *Mez*, 76 Cal. App. 4th at 875, 90 Cal. Rptr. 2d at 734.
56. *See id.* at 877-78, 90 Cal. Rptr. 2d at 736.

Appeal was able to distinguish *Mez Industries* from *Palmer*. However, the California Supreme Court has not yet addressed this issue, and may or may not agree with the Court of Appeal's ruling.

FLORIDA PREPAID v. COLLEGE SAVINGS: UNITED STATES SUPREME COURT SUPPORTS STATE IMMUNITY FROM SUIT UNDER FEDERAL PATENT LAW

Barry N. Young[†] and Rachael A. Campbell[††]

I. INTRODUCTION

In *Florida Prepaid Postsecondary Educ. Expense Bd. v. College Sav. Bank*, ("*Florida Prepaid*")[1] the United States Supreme Court dealt patentees a blow by denying their right to sue states in federal court for patent infringement. *Florida Prepaid* reversed the decision of the Court of Appeals for the Federal Circuit which held that Congress (by amending existing patent law[2]) had validly abrogated the states' sovereign immunity[3] from patent infringement suits pursuant to the authority granted by section 5 of the Fourteenth Amendment.[4] Although Congress had "clearly expressed its intent to abrogate immunity"[5] and had ostensibly acted "pursuant to a valid exercise of power,"[6] the Patent and Plant Variety Protection Remedy Clarification Act ("Patent Remedy Act"[7]) could not be sustained as

---

[†] B.S., M.S. Louisiana State University; J.D. University of Maryland. Mr. Young is a partner at Gray Cary Ware & Freidenrich, LLP, Palo Alto.

[††] B.A, University of Washington; J.D. Candidate, (expected May, 2000) Santa Clara University School of Law. Rachael can be reached at racampbell1@yahoo.com.

1. 119 S. Ct. 2199 (1999).

2. 35 U.S.C. § 271(h) (1992); 35 U.S.C. § 296(a) (1992). Patent and Plant Variety Protection Remedy Clarification Act.

3. State sovereign immunity is granted by the U.S. Constitution. "The Judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by Citizens of another State or by Citizens or Subjects of any Foreign State." U.S. CONST. amend. XI.

4. *Florida Prepaid*, 119 S.Ct. at 2202. *See also* U.S. CONST. amend. XIV, § 5, "The Congress shall have the power to enforce, by appropriate legislation, the provisions of this article."

5. *Florida Prepaid*, 119 S. Ct. at 2204; *see also* Atascadero State Hosp. v. Scanlon, 473 U.S. 234 (1985); Chew v. California, 893 F.2d 331 (Fed. Cir. 1990).

6. *Florida Prepaid*, 119 S. Ct. at 2205; *see also* Seminole Tribe of Florida v. Florida, 517 U.S. 44 (1996).

7. 35 U.S.C. § 271(h) (1992); 35 U.S.C. §296(a) (1992).

"appropriate"[8] legislation enacted to enforce the guarantees of the Fourteenth Amendment's Due Process Clause[9] because Congress had exceeded its authority under section 5 of the Fourteenth Amendment.

II. BACKGROUND

College Savings Bank ("College Savings") marketed and sold certificates of deposit, which were "essentially annuity contracts for financing future college expenses,"[10] and obtained a patent for this financing method.[11] Florida Prepaid Postsecondary Education Expense Board, ("Florida Prepaid") an entity created by the state of Florida, administered similar tuition prepayment contracts.[12] College Savings brought an infringement action[13] against Florida Prepaid pursuant to 35 U.S.C. § 271(a), claiming that Florida Prepaid had directly, indirectly and willfully infringed College Savings' patent.[14]

A. Chew v. California and The Patent Remedy Act

Before discussing *Florida Prepaid,* an understanding of certain prior events will be useful. The Patent Remedy Act was, in part a direct response to the 1990 decision of the Court of Appeals for the Federal Circuit in *Chew v. California* ("*Chew*").[15]

In *Chew*, the patentee (an Ohio resident) brought suit against the state of California alleging infringement of a patented method for testing auto exhaust emissions.[16] Chew alleged that Congress had abrogated state sovereign immunity by use of the term "whoever" in section 271 of the patent statute,[17] and by vesting exclusive

---

8. *Florida Prepaid*, 119 S. Ct. at 2206; *see also* City of Boerne v. Flores, 521 U.S. 507 (1997).

9. *Florida Prepaid*, 119 S. Ct. at 2202. The Due Process Clause of the Fourteenth Amendment provides, "No State shall... deprive any person of life, liberty, or property, without due process of law." U.S. CONST. amend. XIV, § 1.

10. *Florida Prepaid*, 119 S. Ct. at 2202.

11. *See id.*

12. *See id.* at 2203.

13. College Savings filed suit in U.S. District Court for the District of New Jersey. *See id.* at 2203.

14. *See id.*

15. 893 F.2d 331 (Fed. Cir. 1990).

16. *Id.* at 332.

17. 35 U.S.C. § 271(a) provides, in part: "(a) Except as otherwise provided in this title, whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefore, infringes the patent."

jurisdiction in federal courts to decide patent infringement claims.[18] The Federal Circuit rejected both of these arguments, holding that "Congress must express its intention to abrogate the Eleventh Amendment in *unmistakable language in the statute itself,*"[19] and the word "whoever" as used in the statute was too general to evidence Congressional intent to abrogate.[20] The court noted that "the exclusivity of a congressional power or the exclusiveness of the federal court remedy had not been relied upon as grounds or support for abrogation."[21] Due to California's immunity under the Eleventh Amendment, the court affirmed dismissal of Chew's suit for failure to state a claim upon which relief could be granted.[22] The United States Supreme Court later noted the Patent Remedy Act's objective was to clarify that the term "whoever" as used in section 271 included any State, instrumentality of a State, and any officer or employee of a State or instrumentality of a State in the definition of those subject to suit in federal court for infringement of patents and plant variety protections.[23]

B. Seminole Tribe of Florida v. Florida

In 1996, the United States Supreme Court decided *Seminole Tribe of Florida v. Florida* ("*Seminole*")[24]. The impact of this case was later felt severely by College Savings. In *Seminole*, the Court was asked to decide whether the Eleventh Amendment prevented Congress from authorizing suits by Indian tribes against States to enforce legislation enacted pursuant to the Indian Commerce Clause (Article I).[25] The Court answered in the affirmative, holding that although Congress had evidenced a clear intent to abrogate,[26] Article I

18. *See Chew*, 893 F.2d at 333.

19. *Id.* at 334 (emphasis added) (citing Atascadero State Hosp. v. Scanlon, 473 U.S. 234, 243 (1985)).

20. *Id.*

21. *Id.* at 335 (citing Hoffman v. Connecticut Dep't of Income Maintenance, 492 U.S. 96, 100 (1989)).

22. *See id.* at 332.

23. *See Florida Prepaid*, 119 S.Ct. at 2203 (citing Pub. L. No. 102-560 preamble, 106 Stat. 4230).

24. 517 U.S. 44 (1996).

25. *See Id.* at 53 (also discussing whether the doctrine of Ex Parte Young permitted suits against a State's Governor to enforce a provision of the Act in question; an issue beyond the scope of this case note).

26. *See Id.* at 47 (as required by Atascadero State Hosp. v. Scanlon, 473 U.S. 234, 240 (1985)). *See also* Chew v. California, 893 F.2d 331, 333 (Fed. Cir. 1990).

of the Constitution *did not* grant Congress authority to abrogate the States' sovereign immunity.[27]

The Court had previously found "authority to abrogate under only two provisions of the Constitution."[28] These were section 5 of the Fourteenth Amendment,[29] and [in *Pennsylvania v. Union Gas Co.*[30] ("*Union Gas*")] the Interstate Commerce Clause, Article I, section 8, clause 3.[31] The *Seminole* Court overruled *Union Gas* because it "ha[d] created confusion among the lower courts . . . ."[32] Further, the Court explained that "[n]ever before the decision in Union Gas had we suggested that the bounds of Article III could be expanded by Congress, operating pursuant to any constitutional provision other than the Fourteenth Amendment."[33] The Court found no principled distinction between the Indian Commerce Clause and the Interstate Commerce Clause to support abrogation.[34] Thus, after *Seminole*, the sole authority under which Congress could abrogate the states' sovereign immunity was section 5 of the Fourteenth Amendment.

C. City of Boerne v. Flores

Although *Seminole* specifically preserved Congress' authority to abrogate states' sovereign immunity under section 5 of the Fourteenth Amendment,[35] the bounds of Congress' authority were still unclear. In 1997, the Court addressed this issue in *City of Boerne v. Flores* ("*City of Boerne*").[36] *City of Boerne* considered "whether the [Religious Freedom Restoration Act ("RFRA")] . . . was a proper exercise of Congress' § 5 power 'to enforce' by 'appropriate legislation' the constitutional guarantee that no State shall deprive any person of 'life, liberty or property, without due process of law' . . . ."[37] The Court held the RFRA could not withstand constitutional

27. *See id.* at 47.
28. *Id.* at 59.
29. *See id.*
30. 491 U.S. 1 (1989) (plurality opinion).
31. Seminole Tribe of Florida v. Florida, 517 U.S. 44, 59 (1996) (citing *Union Gas*, 491 U.S. at 19-20.).
32. *Id.* at 64.
33. *Id.* at 65.
34. *See id.* at 63.
35. *See id.* at 59.
36. 521 U.S. 507 (1997).
37. *Id.* at 517.

scrutiny.[38]

Reiterating that the remedial nature of Congress' power under section 5 extended "only to 'enforcing' the provisions of the Fourteenth Amendment,"[39] the Court acknowledged that distinctions between measures that remedy or prevent unconstitutional actions and those that make a substantive change in governing law must be observed.[40] The Court stated that appropriateness is determined by "congruence and proportionality between the injury to be prevented or remedied and the means adopted to that end."[41] It held that for Congress to invoke section 5, it must identify conduct transgressing the Fourteenth Amendment's substantive provisions, and must tailor its legislative scheme to remedying or preventing such conduct.[42]

III. DISCUSSION

A. Procedural History

Thus, the stage was set for *Florida Prepaid.* When College Savings filed suit in 1994, the Patent Remedy Act was in effect.[43] After *Seminole* was decided in 1996, Florida Prepaid moved to dismiss on grounds of sovereign immunity, arguing that the "Patent Remedy Act was an unconstitutional attempt by Congress to use its Article I powers to abrogate state sovereign immunity."[44] College Savings responded that "Congress had properly exercised its power pursuant to section 5 of the Fourteenth Amendment to enforce the guarantees of the Due Process Clause in section 1 of the Amendment."[45] The district court agreed with College Savings and denied Florida Prepaid's motion to dismiss; and the Federal Circuit affirmed.[46] The Supreme Court granted certiorari to determine whether the Patent Remedy Act validly abrogated the States' sovereign immunity, and reversed.[47]

---

38. *See id.* at 536.
39. *Id.* at 519.
40. *See id.* at 519-20.
41. *Id.* at 520.
42. *See City of Boerne*, 521 U.S. 507, 520 (1997).
43. *See Florida Prepaid*, 119 S. Ct. at 2203.
44. *Id.* at 2204.
45. *Id.*
46. *Id.* Federal Circuit decision reported at 148 F.3d 1343 (Fed. Cir. 1998).
47. *Florida Prepaid*, 119 S.Ct. at 2204.

B. The Majority

The Court began its examination with the same two-part inquiry utilized in *Seminole*.[48] First, it considered whether Congress had unequivocally expressed its intent to abrogate the states' immunity in the Act.[49] The Court agreed with the parties and the Federal Circuit that, "in enacting the Patent Remedy Act, Congress made its intention to abrogate the states' immunity 'unmistakably clear in the language of the statute.'"[50] Next the Court considered whether Congress had acted pursuant to a valid exercise of power.[51] Congress justified the Patent Remedy Act on three sources of Constitutional authority: "the Patent Clause, Art. I, § 8 cl. 8; the Interstate Commerce Clause, Art. I, § 8, cl. 3; and § 5 of the Fourteenth Amendment."[52] Since *Seminole* held that Congress did not have the authority to abrogate the states' sovereign immunity under Article I powers, the Patent Remedy Act could be sustained, if at all, only under section 5 of the Fourteenth Amendment. The Court noted that *Seminole* specifically reaffirmed that "Congress retains the authority to abrogate state sovereign immunity pursuant to the Fourteenth Amendment,"[53] and proceeded with its Due Process analysis.

The Court conceded that a patent is a form of property, and is properly included in the protections of the Due Process Clause.[54] The Court also agreed with College Savings that, appropriate legislation pursuant to the Enforcement Section (section 1) of the Fourteenth Amendment could abrogate state sovereignty.[55] However, the legislation must be "appropriate" under section 5 as that term was construed in *City of Boerne*.[56] "Appropriateness" is determined by first identifying conduct that transgresses the Fourteenth

48. *See id.* at 2205 (Chief Justice Rehnquist wrote for the majority).

49. *See id.*

50. *Id.* at 2205 (citing Dellmuth v. Muth, 491 U.S. 223, 228 (1989)).

51. *See id.*

52. *Id.*

53. *Id.*

54. In a related case decided the same day (*College Sav. Bank v. Florida Prepaid Postsecondary Educ. Expense Bd.*, 119 S. Ct. 2219 (1999) the Court held the Trademark Remedy Clarification Act was not a valid abrogation of sovereign immunity; Florida had not waived its immunity by its activities in interstate commerce; and, the "property rights" asserted by College Savings (a right to be free of a business competitors false advertising and a more generalized right to be secure in one's business interests) *did not* rise to the level of property rights protected by the Due Process Clause.

55. *See Florida Prepaid*, 119 S. Ct. at 2206.

56. *See id.*

Amendment's substantive provisions, then tailoring legislation to remedy or prevent such conduct.[57] If the legislation is so out of proportion to a supposed remedial or preventive object that it cannot be understood as responsive to or designed to prevent unconstitutional behavior, it cannot stand.[58]

The underlying conduct at issue in *Florida Prepaid* was state infringement of patents and the use of sovereign immunity to deny patent owners compensation for infringement.[59] The Court noted that it was not the infringement itself by state action that was unconstitutional, but the deprivation of a constitutionally protected property interest without due process of law.[60] The Court found that Congress had not identified a pattern of patent infringement by the states, "let alone a pattern of constitutional violations,"[61] and noted this "lack of evidence" compared to the undisputed record of racial discrimination in voting rights cases.[62] The Court conceded that state infringement of a patent rises to the level of a constitutionally protected interest, but held there is no constitutional violation unless *the State provides no remedy, or only inadequate remedies.*[63] Despite evidence in the record that Congress had considered the uncertain availability of state law remedies, the Court noted that "the primary point . . . was not that state remedies were constitutionally inadequate, but rather that *they were less convenient than federal remedies and might undermine the uniformity of patent law.*"[64] The Court also dismissed a concern that a patchwork of state laws would undermine the goal of national uniformity. It stated that "the need for uniformity in the construction of patent law is *undoubtedly important,* but that is a factor which belongs to the Article I patent-power calculus . . ."[65] However, after *Seminole,* Article I did not grant Congress the power to enact such legislation.[66]

The Court next quoted precedent to support its view that a state actor's *negligent* act that causes unintended injury to a person's

57. *See id.* at 2207.
58. *See id.* (citing City of Boerne v. Flores, 521 U.S. 507 (1997)).
59. *See id.*
60. *See id.* at 2208.
61. *Florida Prepaid,* 119 S.Ct. at 2207.
62. *See id.*
63. *See id.* at 2208.
64. *Id.* at 2209 (emphasis added).
65. *Id.* (emphasis added).
66. *See id.* at 2211.

property does not deprive that person of property within the meaning of the Due Process Clause.[67] Although the Court appeared to acknowledge the strict liability nature of patent infringement,[68] it found scant support in the record for Congress' conclusion that states were depriving patent owners of due process of law by pleading sovereign immunity in federal court patent actions.[69] The Court noted, "[t]he legislative record thus suggests that the Patent Remedy Act does not respond to a history of 'widespread and persisting deprivation of constitutional rights' of the sort Congress has faced in enacting proper prophylactic § 5 legislation."[70] Rather, the Court found that Congress had enacted the Patent Remedy Act in response to "a handful of instances of state patent infringement that do not necessarily violate the Constitution."[71]

The Court observed that Congress did nothing to limit the coverage of the Act to cases involving arguably constitutional violations, such as where a state refuses to offer any state-court remedy, or limit the remedy to nonnegligent infringement, to infringement pursuant to state policy, or against states with questionable remedies.[72] Therefore, the Court held Congress could not validly rely on the Fourteenth Amendment's authorization of "appropriate legislation" to abrogate state sovereign immunity.[73] Essentially, the Court felt that Congress overreached its authority by not limiting the Patent Remedy Act to situations involving clear failure by the states to provide remedies for patent infringement.

C. The Dissent

The dissent[74] viewed the Patent Remedy Act as an appropriate exercise of Congress' power under section 5[75] for three principle reasons. First, there was adequate evidence of due process violations based upon the absence of effective state remedies for patent

67. *See Florida Prepaid*, 119 S.Ct. at 2209.

68. *See id.* (citing 5 DONALD S. CHISUM, CHISUM ON PATENTS § 16.02, at 16-31 (rev. ed. 1998)).

69. The Federal Circuit opinion had identified only eight patent infringement suits against states in the 110 years between 1880 and 1990. *See id.* at 2207.

70. *Id.* at 2210 (citing City of Boerne v. Flores, 521 U.S. 507, 526 (1997)).

71. *Id.*

72. *See id.* at 2210.

73. *Florida Prepaid*, 119 S.Ct. at 2210-11.

74. Justice Stevens, joined by Justices Souter, Ginsburg and Breyer filed the dissenting opinion. *See id.* at 2211.

75. *See id.*

infringement by states.[76] Second, Congress had sufficient evidence of heavy state involvement in the patent system,[77] and the Patent Remedy Act merely put the states in the same position as private users of the patent system, as well as in substantially the same position as the United States itself.[78] Finally, the dissent emphasized the need for national uniformity in the patent system,[79] and the long-time statutory pre-emption of state jurisdiction over patent infringement cases.[80]

The dissent criticized the majority for failing to answer the real question, i.e., whether the Patent Remedy Act may be applied to willful infringement,[81] arguing the majority had ignored the facts of the case.[82] Looking to the majority's reasoning based on perceived deficiencies in the evidence reviewed by Congress before enacting the Patent Remedy Act,[83] the dissent stated: "[I]t is quite unfair for the Court to strike down Congress' Act based on an absence of findings supporting a requirement this Court had not yet articulated.[84] The legislative history . . . makes it abundantly clear that Congress was attempting to hurdle the then-most-recent barrier this Court had erected . . ."[85] The dissent was referring to the "clear statement" rule of *Atascadero* and *Chew*, decisions to which the Patent Remedy Act responded. Congress *had* heard testimony about inadequate state remedies[86] (as required by *City of Boerne*), and found that states and their instrumentalities were heavily involved in the patent system, and that "state infringement of patents was likely to increase."[87] The dissent found it particularly ironic that the majority relied on lack of evidence of state remedies given the fact that Congress had long ago pre-empted state jurisdiction over patent infringement cases.[88] Furthermore, even if "such remedies might be available in theory, it

76. *See id.* at 2217.

77. *See id.* at 2215 n.8.

78. *See Florida Prepaid*, 119 S. Ct. at 2218.

79. *See Florida Prepaid*, 119 S.Ct. at 2211-13.

80. *See id.* at 2216.

81. *See id.* at 2213.

82. *See id.* at 2214.

83. *See id.* at 2214.

84. *See* The Patent Remedy Act was enacted in 1992, but *City of Boerne* was not decided until 1997.

85. *Florida Prepaid*, 119 S. Ct. at 2214.

86. *See id.*

87. *Id.* at 2215.

88. *Id.* at 2216.

would have been 'appropriate' for Congress to conclude that they would not guarantee due process in infringement actions against state defendants."[89] The dissent argued that state judges have never had exposure to patent litigation and, unlike infringement actions brought in federal district court, their decisions would not be reviewable by the Court of Appeals for the Federal Circuit.[90] The dissent concluded *City of Boerne* amply supported congressional authority to enact the Patent Remedy Act, whether one assumed state infringement to be scarce or widespread.[91]

Furthermore, the dissent argued persuasively that Congress had sufficient evidence of due process violations before it to meet the standard expressed in *City of Boerne*.[92] The RFRA had sought to change the meaning of the Free Exercise Clause, not to remedy or prevent violations of the Clause as the Court had interpreted it.[93] The Patent Remedy Act, "was Congress' attempt to prevent violation of due process based upon a substantiated fear that states would be unable or unwilling to provide adequate remedies for their own violation of patent-holders rights."[94] In *City of Boerne*, there was no congruence between the means used and ends achieved because of the sweeping nature of the statute. However, the sole purpose of the Patent Remedy Act was to abrogate state sovereign immunity as a defense to a charge of patent infringement.[95] It had no impact whatsoever on any substantive rule of state law, but merely effectuated federal policy to confine patent litigation to federal judges.[96] As a result, the dissent found that sufficient congruence existed between the means used and the end achieved to justify Congress' action as an appropriate exercise of power under section 5 of the Fourteenth Amendment.[97]

Finally, the dissent emphasized the importance of national uniformity in patent law as a long-standing proposition. Justice Story said of the Patent and Copyright Clauses to the Federal Constitution, "[i]t is beneficial to all parties, that the national government should

89. *Id.*
90. *See id.* at 2216.
91. *See Florida Prepaid*, 119 S.Ct. at 2216.
92. *See id.* at 2217.
93. *See id.*
94. *Id.*
95. *See id.* at 2218.
96. *See id.* at 2218.
97. *See Florida Prepaid*, 119 S.Ct. at 2218.

possess this power; . . . [because authors and inventors would otherwise] be subjected to the varying laws and systems of the different states . . . which would impair, and might even destroy the value of their rights . . . ."[98] The dissent argued, "sound reasons support both Congress' authority over patents and its decision in 1800 to vest exclusive jurisdiction over patent infringement litigation in the federal courts."[99] For example, the substantive law applied in patent infringement cases is entirely federal; there is a strong federal interest in a uniform interpretation of patent statutes; and patent infringement litigation is often technical, raising issues unfamiliar to the average trial judge.[100] In fact, that consideration as well as divergence among the federal circuits in their interpretation of patent issues gave rise to the congressional decision to consolidate appellate jurisdiction in the Court of Appeals for the Federal Circuit.[101] The dissent also criticized the majority's comment that the need for uniformity is a factor which belongs to the Article I patent-power calculus; asserting that Article I is directly relevant because it establishes the constitutionality of the basic congressional decision to vest exclusive jurisdiction over patent infringement cases in the federal courts.[102] According to the dissent, this basic decision was "unquestionably appropriate," therefore, "it was equally appropriate for Congress to abrogate state sovereign immunity in patent infringement cases."[103]

IV. CONCLUSION

Florida Prepaid will undoubtedly have far-reaching impact for patentees. Patentees now occupy a very precarious position relative to the states, and are left with the prospects of no uniform, viable forum for addressing state violation of their property rights. This is particularly true after the Court's decision in *Alden v. Maine*.[104] At least one district court has attempted to circumvent *Florida Prepaid*; in *New Star Lasers v. Regents of the Univ. of Cal.* ("*New Star*")[105] the court held that a state university's Eleventh Amendment immunity

98. *Id.* at 2211-12.

99. *Id.* at 2212.

100. *See id.*

101. *See id.*.

102. *See id.* at 2213.

103. *Id.*

104. 119 S. Ct. 2240 (1999) (Congress may not subject a state to suit in *state* court, without its consent).

105. 63 F. Supp. 2d 1240 (E.D Cal. 1999).

was waived by its acquisition of a patent. *New Star* referred to the companion case to *Florida Prepaid*,[106] which held that the doctrine of constructive waiver as set out in *Parden v. Terminal R. Co. of Ala. Docks Dep't*,[107] was overruled, but confirmed the proposition that, "Congress can compel a waiver where the State seeks not merely to engage in 'otherwise lawful activity' but rather receives a 'gift or gratuity' or 'federal beneficence' that Congress may rightfully withhold."[108] The *New Star* court held that since a patent is a unique form of nationally recognized intellectual property created by Congress pursuant to its authority under the Patent Clause, it constituted a "gift or gratuity" bestowed by the federal government.[109] Therefore, if Congress conditions the receipt of such a gift on a waiver of Eleventh Amendment immunity, then Congress has acted permissibly.[110] To date, *New Star* stands but has been criticized, "Justice Shubb appears to be climbing out on a limb in reading the Patent Remedy Clarification Act of 1992 as a forced waiver statute rather than an abrogation statute."[111] Ultimately, it is doubtful that the reasoning of *New Star* will stand.

Until Congress reacts to *Florida Prepaid* with another attempt to meet the criteria articulated by the Court for abrogation of state sovereign immunity, patentees are left with the option of convincing a state to waive its immunity to suit in federal court or articulating a viable state law theory to assert in state court. Neither advances the public policy of promoting the progress of science and the useful arts in Article I, section 8 of the Constitution.

106. College Sav. v. Florida Prepaid Postsecondary Educ. Expense Bd., 119 S. Ct. 2219 (1999) (holding that the Lanham Act did not apply to state trademark infringement).

107. 377 U.S. 184 (1964).

108. *New Star*, 63 F. Supp. 2d at 1243.

109. *See id.* at 1244.

110. *See id.*

111. *State University Waived Immunity From Suit to Declare Patent Invalid*, 58 Pat., Trademark & Copyright J. (BNA) No. 1442, at 595 (Sept. 23, 1999).