University of Dayton Law Review

Volume 25
Number 1 *25th Anniversary Edition*

Article 8

10-1-1999

The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technology

Caitlin Garvey
University of Dayton

THE NEW CORPORATE DILEMMA: AVOIDING LIABILITY IN THE AGE OF INTERNET TECHNOLOGY

Caitlin Garvey[*]

TABLE OF CONTENTS

"The Internet is a rapidly developing technology – today's problems may soon be obsolete while tomorrow's challenges are, as yet, unknowable."[1]

I. INTRODUCTION

The technological developments of recent years have been both a blessing and a curse for corporate America. While new advances have helped to improve the bottom line, they have also created numerous potential liability concerns. The Internet has served as a primary source of these increased concerns. As corporations increase employee access to the Internet, this access to information increases the potential for employee

---

[*] Executive Editor, 1999-2000, University of Dayton Law Review. J.D. expected, May 2000, University of Dayton School of Law; M.A., 1994, Wright State University; B.A., 1991, Saint Mary-of-the-Woods College.

[1] David R. Sheridan, Zeran v. AOL *and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 166 (1997).

computer abuse. With the push of a button, employees can distribute confidential records worldwide in a matter of minutes,[2] peruse pornography over the Internet from their office computer,[3] or send sexually harassing messages via e-mail, chat rooms, or newsgroups.[4] Thus, the increased use of technology also increases employers' worries regarding potential liability from other employees and third parties injured by employee computer abuse.

While employer liability for acts of an employee is generally measured under the doctrine of *respondeat superior*,[5] the rise in corporate Internet use and the way corporations connect to the Internet has exposed a new area of potential liability, that of an Internet Service Provider ("ISP"). This new area of potential liability is shrouded in ambiguity because of the contradictory language in statutory definitions for Internet technology.[6] The ambiguity is further increased by the fact that because the issue of whether corporations who function like traditional ISPs are legally defined as ISPs has yet to be specifically addressed.

---

[2] James Garrity and Eoghan Casey, *Internet Misuse in the Workplace: A Lawyer's Primer*, FLA. B. J., Nov. 1998, at 24-25.

[3] *Id.* Media Metrix, an Internet traffic analysis company, states that nineteen percent of employees visit pornographic sites, compared to 69 percent for news or information sites. Maria Seminerio, *Surfing for Smut on the Clock*, ZDNN News Channel (visited Oct. 20, 1999) <http://www.zdnet.com/zdnn/content/pcwk/1447/pcwk0095.html>. Likewise, a 1997 Nielsen Media Research study reported that employees at IBM, AT&T, and Apple Computer, Inc. made 13,000 workplace visits in a month to the Penthouse magazine Internet site. *Id.*

[4] *Id.* The nature of e-mail can disguise actions that would be obvious if carried out in person, as in an employee who could not unobtrusively make almost fifty trips to a colleague's desk in a week but who could send the same amount of e-mail messages without drawing attention to himself. Lisa Stansky, *Changing Shifts: Does Anyone Still Work Here? As More Jobs Move from the Traditional '9 to '5 Alternative Workstyles are Forcing Redefinitions of Employment Law*, 83 A.B.A. J., Jun. 1997, at 58.

[5] Generally, employer liability is measured under the doctrine of respondeat superior, and employers' abilities to control employee behavior have been carefully balanced against the employees' reasonable expectations of privacy. Laurie Thomas Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"*, 28 J. MARSHALL L. REV. 139, 155 (Fall 1994); Jarrod J. White, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1088 (Spring 1997); Stuart Rosove, *Employee Internet Use and Employer Liability*, 1997 ANDREWS EMPLOYMENT LITIG. REP. 22106 (Apr. 8, 1997). The Electronic Communications Privacy Act ("ECPA") prohibits interception and disclosure of messages by outside intruders, such as employers who are neither parties to the communication nor a part of the transmission process, and regulates similar interception by law enforcement agencies. 18 U.S.C. § 2511 (1999); S. REP. NO. 99-541, at 2 (1986). However, the ECPA contains exceptions that employers have successfully relied upon to argue that they may lawfully monitor their employees: 1) interception by the sender or recipient of a message in transmission; 2) interception with the consent of the sender or recipient; and 3) monitoring in the normal course of business, when necessary to protect rights or property of the network provider. 18 U.S.C. § 2511 (1998).

[6] *See infra* notes 24-34 and accompanying text.

This Comment asserts that corporations whose direct connections to the Internet mirror those of traditional ISPs are indeed ISPs despite the lack of statutory guidelines. After providing a background of recent statutory Internet definitions,[7] this Comment analyzes the nature of corporate Internet connections.[8] Using the Communications Decency Act ("CDA") and the Digital Millennium Copyright Act ("DMCA") as a framework for analyzing Congressional treatment of ISPs, this Comment further proposes that as ISPs, these corporations should receive some level of immunity from users' computer abuse similar to the immunity received by traditional ISPs.[9] However, the CDA and the DMCA indicate that corporate ISP immunity is conditioned on the establishment of "acceptable use" policies to limit computer abuse.[10] This Comment's final section analyzes these policies and discusses how, despite the unsettled nature of this issue, it appears that corporate ISPs can attain immunity from liability by implementing computer policies ("acceptable use" policies) and instituting monitoring programs.[11] This Comment concludes that statutes such as the CDA and the DMCA indicate that corporations with direct Internet connections are in a unique situation of having ISP status, but the benefits of that status are conditioned on using the employer role to monitor that technology.[12]

II. BACKGROUND

A. The Internet Explosion in Corporate America

As millions of people adopt the Internet as an essential component of their daily lives,[13] many companies have realized the Internet's potential in

---

[7] *See infra* notes 24-34 and accompanying text.

[8] *See infra* notes 35-60 and accompanying text.

[9] *See infra* notes 61-130 and accompanying text.

[10] *See infra* notes 61-130 and accompanying text.

[11] *See infra* notes 131-68 and accompanying text.

[12] *See infra* note 169 and accompanying text.

[13] Frank Gens, *IDC Predictions '99: The "Real" Internet Emerges*, IDC BULLETIN #17971 (Dec. 1998) (visited Nov. 8, 1999) <http://www.idc.COM/EI/content/123198EI.htm>. The United States is currently estimated to have over 100 million Internet users. *U.S. Tops 100 Million Internet Users According to Computer Industry Almanac* (Nov. 1999) (visited Jan. 11, 2000) <http://weblib.lkg.dec.com/Newscast/199911/08/19991108143651 31PR.HTM>. Furthermore, it is thought that the Internet will have over 490 million users by the end of 2002 and over 765 million users by the end of 2005. *Id.* The International Data Corporation (IDC) reports that Internet commerce will exceed one trillion dollars by 2003, with users who purchase products over the Internet moving

the corporate sector.[14] These companies revamped their corporate network to provide Internet services internally through an Intranet[15] (an internal World Wide Web site) in hopes of seeing corporate improvements.[16] As nearly eighty-seven percent of all companies already use Intranets,[17] Intranets are becoming a critical component of corporate business.[18]

Although corporate Intranets can exist solely within the company, most corporations choose to link their private Intranet to the public Internet.[19] These corporations realize that the Intranet's communication benefits expand if one corporation's Intranet is shared with a partner corporation's Intranet with the Internet between them.[20] Likewise, corporations linked to the Internet can provide better customer service to customers through e-mail or the World Wide Web.[21] Internet commerce also provides new corporate possibilities with predictions suggesting that Internet commerce will more than double in 1999 to 68 billion dollars and that buyers will

---

from 31 million in 1998 to more than 183 million by 2003. *Internet Commerce Will Rocket to More than $1 Trillion by 2003, According to IDC*, IDC (visited Oct. 20, 1999) <http://www.idc.com/Data/Internet/content/NET062899PR.htm>.

[14] MELANIE HILLS, INTERNET BUSINESS STRATEGIES 5-8 (1997).

[15] *Id.* An Intranet is a network based on TCP/ICP protocols (an Internet) of a corporation, accessible only by the corporation's employees or others with authorization. An Intranet's World Wide Web sites look and act like other World Wide Web sites, but the firewall surrounding the Intranet fends off unauthorized access. ZDNet, *ZDNet Webopaedia* (visited Oct. 20, 1999) <http://www.zdwebopedia.com/TERM/i/intranet.html>. The term "intranet" started being used in 1995 to refer to these corporate internets, replacing terms such as internal webs, internet clones, corporate webs, or private webs. HILLS, *supra* note 14, at 6.

[16] HILLS, *supra* note 14, at 5-8.

[17] Jeffrey Schwartz & Richard Karpinski, *Intranets Grow Up(scale)*, INTERNETWEEK, Dec. 29, 1998.

[18] HILLS, *supra* note 14, at 5-8. Intranets assist companies by improving productivity and shortening product development time since employees have quick and easy access to needed information. *Id.* at 6-8. EDS's Intranet includes accounting policies, product catalogs, employee benefits information, job postings, competitor profiles, Internet newsgroups, and EDS internal newsgroups. *Id.* at 145-48. Intranets also improve internal communications while cutting communications costs. *Id.* at 31-35. For example, HarperCollins previously printed and distributed a paper-based corporate directory but now uses an online phone book through the corporation's Intranet. *Case Study for HarperCollins*, Microsoft Intranet Solutions at 2 (on file with author).

[19] HILLS, *supra* note 14, at 6.

[20] *Id.* at 6.

[21] *Id.* at 25. For example, AT&T allows customers to access their bills and plans to eventually allow customers to connect to its Intranet to do things such as setting up their own 800-number trees. *Id.* In addition, Microsoft reported a decrease in phone volume after it instituted "Support Online" as part of its Intranet, thereby saving customers a telephone call while providing easy access to technical information they need. *Backstage, Operating microsoft.com.*, Microsoft.com (visited Feb. 20, 1999) <http://www.microsoft.com/misc/backstage/bkst_cs_supportonline.htm>. The site has 129,000 visitors per day, and telephone calls have dropped from 35,000 inquiries each day in August 1995 to fewer than 20,000 calls each day. *Id.*

spend nearly 900 billion dollars online from 1999 through 2002.[22] Consequently, these companies have Internet gateways to directly connect their Intranets to the Internet.[23] As these corporate links to the Internet become customary, the critical questions are whether these corporations connecting to the Internet are also ISPs, and, if so, does that ISP status change these corporations' liability concerns regarding employee computer abuse?

B. Statutory Development of ISP Terminology

Legal definitions for Internet technology struggle to match the Internet's rapid technological development.[24] Among the computer industry, terminology for Internet technology is nebulous, with numerous terms referring to the same function and some terms containing several meanings.[25] Indeed, the terminology indicates a "functional" approach to the technology, as the term "ISP" is used for a variety of different types of access and services to the Internet, which is, at its foundation, a mass of connections with the ISPs providing the connections from the Internet to the customer.[26] The total number of entities under the encompassing heading of "ISP" has grown from about 1500 in 1996 to more than 6500,[27] and it is estimated that the number of ISPs will rise five-fold in five years.[28]

The term ISP describes providers that offer access to the Internet (traditionally called Internet Access Providers) and providers that operate Internet servers and provide Internet services (such as e-mail, Web page hosting, or Usenet newsgroups to subscribers).[29] Occasionally, some

---

[22] Gens, *supra* note 13.

[23] HILLS, *supra* note 14, at 6, 10-11.

[24] Connecting corporations to the Internet has become widespread with the bulk of new business applications released in 1998 offering some level of World Wide Web connectivity, and estimates suggest that the 100,000 Intranet-web servers in 1995 will grow to 4.7 million by the advent of the Millennium. Schwartz, *supra* note 17; HILLS, *supra* note 14, at 8 (citing Ian Campbell, Director of Collaborative Technologies for International Data Corporation). Even smaller companies have realized the value of accessing the Internet, as estimates indicate that by 2002 small business will form 20 to 25 percent of the online presence and that one in eight United States small businesses will have a Web site by the end of 1999. Gens, *supra* note 13.

[25] Timothy L. Skelton, *Internet Copyright Infringement and Service Providers: The Case for a Negotiated Rulemaking Alternative*, 35 SAN DIEGO L. REV. 219, 227, n. 30 (1998).

[26] UUNet, *Connection Guide*, (visited Jan. 11, 2000) <http://www.uunet.com.html>.

[27] Seth Lubove & Anne Linsmayer, *Mom and Pops Thrive . . . .*, FORBES, Feb. 22, 1999, at 120.

[28] *Id.* at 121.

[29] Internet Access Providers ("IAPs") traditionally only provide access to content located on servers outside its system. Because an IAP has no physical access to the information residing on servers located outside its system, it has neither the right nor the ability to control that content.

distinctions are made among ISPs, with major telecommunications providers such as AT&T and UUNet labeled "Internet backbone providers" or "major telecommunication companies." Generally, however, the term ISP encompasses all organizations that provide Internet-related services.[30]

Although statutory definitions appear to mirror those of the industry by embracing a broad, functional approach to ISPs, the statutory definitions persist in using multiple terms for ISPs. For example, the Communication Decency Act of 1996 uses the term "interactive computer service" to refer to "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[31]

Likewise, the Internet Taxation Freedom Act of 1998 uses the term "Internet Access Service" to define what the computer industry would call an ISP, although Congress specifically excluded the major telecommunication providers from the definition.[32] Congress defined "Internet Access Service" as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services."[33]

In addition, the Digital Millennium Copyright Act ("DMCA") uses the term "service provider" to refer to "an entity offering the transmission, routing, or providing of connections for digital online communications,

---

However, this definition is too limited because IAPs often provide more than simple access to the Internet, and operate servers to give subscribers basic Internet services. Thus, the term ISP is a more accurate description of IAPs. Skelton, *supra* note 25 at 227.

[30] Skelton, *supra* note 25 at 227. The term ISP may have other meanings, as there are many different organizations that provide Internet-related "services." A provider supplying Web site hosting is often referred to as an Internet presence provider (IPP). The regional and national commercial networks that supply network access points to IAPs are also called "service providers." Finally, the system operators of Internet services are also sometimes referred to as service providers. *Id.*

[31] 47 U.S.C. § 230(f)(2) (1998). The CDA's foray into Internet terminology was followed by *ACLU v. Reno* which provided the most recent judicial findings regarding the Internet. 929 F. Supp. 824 (E.D. Pa. 1996). *Reno* carefully outlined the foundational precepts of the Internet. *Id.* at 831-33. Like the CDA, *Reno* did not follow industry terminology for ISPs but used the term ISP to refer to commercial and non-commercial providers that offer modem telephone access to a computer linked to the Internet. *Id.* at 833. The court made a distinction between ISPs and the commercial "online services" such as America Online. *Id.* Furthermore, the court also listed bulletin board systems, direct connections provided by education institutions and corporations, community networks, and access provided by libraries as methods of connecting to the Internet. *Id.*

[32] 47 U.S.C. § 151(3)(D) (1999).

[33] *Id.*

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."[34]

These statutes emphasize the legislature's growing awareness of the Internet as an entity requiring legal regulation while highlighting the difficulty of statutorily defining an ISP. The lack of consistency forces corporations with direct Internet connections to analyze existing definitions to determine how Congress would define their situation. Corporations with direct Internet connections can attain insight into how they fit into the current statutory definitions, particularly by studying the CDA and the DMCA, but those conclusions must be cautiously grounded in an awareness of Congress' failure to specifically address this issue.

III. ANALYSIS

Corporations with direct Internet connections meet the functional definition of an ISP.[35] Although ambiguity exists among current statutory Internet definitions, and no statute specifically addresses corporations with direct Internet connections, Congress' functional approach to the Internet as evidenced in the CDA and the DMCA indicates that corporations with direct Internet connections are indeed ISPs and, therefore, should receive immunity from employee computer abuse.[36]

However, that immunity appears to be conditional, because the CDA and DMCA reflect competing desires for increased technology and decency within that technology.[37] Congress' prevailing goal is to promote Internet technology.[38] Hence, ISPs whose business relationship with subscribers makes monitoring content possible, but extremely difficult, receive extensive immunity for computer abuse.[39] However, ISPs whose relationships with users are conducive to monitoring, such as the employer/employee relationship, receive immunity that is conditional, in some respects, on controlling content.[40] Because corporations' positions as employers and certain exceptions of the Electronic Communications

---

[34] 17 U.S.C. § 512(k)(1)(A) (1998).

[35] *See infra* notes 42-60 and accompanying text.

[36] *See infra* notes 61-130 and accompanying text.

[37] 17 U.S.C. § 512(k)(1)(A) (1998).

[38] Congress stated that it is "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." 47 U.S.C. § 230(b)(2) (1998).

[39] *See infra* notes 61-130 and accompanying text.

[40] *See infra* notes 61-130 and accompanying text.

Privacy Act ("ECPA")[41] permit control of content, immunity is likely conditioned on the institution of "acceptable use" computer policies and monitoring programs.

A. Employers with Direct Internet Connections as ISPs

Corporations that directly connect their Intranet to the Internet have not merely tapped into new technology but have become ISPs. This label would surprise many corporations, who are unaware of Congress' and the computer industry's broad, functional approach to ISPs. Indeed, many people are unaware of the variety of the services offered under the all-encompassing term "ISP." Smaller ISPs actually are reselling services and access provided to them by larger ISPs who link to even larger ISPs (referred to as major telecommunication providers or Internet backbone providers) to connect to the Internet.[42] The smaller ISPs are merely resellers from the larger ISPs, providing companies with web servers, e-mail, domain names, and web access, as well as the final phone connection (or wire) to the Internet, which the larger ISP provides.[43]

A corporation choosing to link its Intranet to the Internet can buy packaged services from an ISP, often buying web servers, e-mail, and domain names.[44] For example, PSINet has numerous corporate accounts paying approximately 500 dollars a month for Internet access, web hosting, security, and other services.[45] Often, corporations that select these packaged services are smaller or medium-sized corporations lacking the capital, staffing, and expertise to implement and maintain an internal system.[46]

---

[41] *See supra* note 5 and accompanying text. The consent and provider exceptions would both suffice, although the consent exception is the prevalent method used by employers. *See supra* note 5 and accompanying text.

[42] E-mail from Gordon Strong, Senior Solutions Architect to Jeff Dunkelberger, Compaq Computer Corporation Senior Consultant (Feb. 8, 1999) (on file with author).

[43] *Id.* For instance, America Online ("AOL") has 15 million paying subscribers, its own browsers and Web site, but lacks its own wires, which it purchases from a larger ISP. Rita Koselka, *Cyberspace: Going Into Orbit*, FORBES, Feb. 22, 1999, at 53. Likewise, Pennsylvania Online pronounced itself an ISP when it started as one server, some modems, and two leased lines from the local telephone company. Seth Lubove & Anne Linsmayer, *Mom and Pops Thrive . . . .*, FORBES, Feb. 22, 1999, at 120.

[44] E-mail from Gordon Strong, Senior Solutions Architect to Jeff Dunkelberger, Compaq Computer Corporation Senior Consultant (Feb. 8, 1999) (on file with author).

[45] Nikhil Hutheesing, . . . *as a Big Guy Mulls Its Fate*, FORBES, Feb. 22, 1999, at 121-22.

[46] Mark Levitt & Mike Comiskey, *Messaging and Collaboration User Survey*, IDC REPORT #17558 (Dec. 1998) (visited Jan. 23, 1999) <http://weblib.lkg.dec.com/IDC/17558-01.htm>. The smaller companies select services from either the large ISPs or the consumer-oriented, smaller ISPs.

Corporations with extensive Intranets may not require the e-mail, web server, or web access that the smaller ISP offers. Instead, they may need some of those services and the telephone connection (the "wire") to the Internet, or they might only need the "wire."[47] Thus, large corporations with developed Intranets often only purchase the "wire" from the major telecommunication company because the corporation already offers the rest of the services that the smaller ISPs provide.[48] As noted by one major telecommunication company, direct corporate Internet access is the next major development in Internet connections, "[w]e're starting to cross the threshold where a different business model makes sense."[49]

These large corporations connect directly to the Internet after purchasing the wire from a large ISP (also called a major telecommunication provider), such as UUNet, Qwest, or AT&T.[50] For example, Compaq Computer Corporation ("Compaq") runs its own Intranet with a domain name system, news, web, and e-mail that is interconnected with its public Internet web pages via a firewall.[51] Compaq connects directly to the Internet through a major telecommunications provider and states that there

---

Depending on their location, it is conceivable that they can be doing business with their local telephone company. E-mail from Gordon Strong, Senior Solutions Architect to Jeff Dunkelberger, Compaq Computer Corporation Senior Consultant (Feb. 8, 1999) (on file with author).

[47] *See* UUNet, *Connection Guide* (visited Feb. 9, 1997) <http://www.uunet.com.html>. Telephone connection possibilities are extensive, as connections to the Internet are available in varieties that range from low-speed, intermittent access to high-speed, permanent connections. *Id.* Companies with Intranets whose Web site is accessible to the public typically chose a dedicated, high-speed link, such as a "T1" or "T3." *Id.* Companies can also choose services such as a unique domain name for the site, Internet (web) servers on the company's local computers, "mailbagging" service to deliver Internet mail to the company's on-site mail server, newsreading sessions, connectivity support, services support, and firewall security. *Id.*

[48] The "wire" is a slang term to describe a T1 or T3 phone wire; rates for T1 services offered by traditional carriers generally range from 1500 dollars to 2000 dollars per month, although competition is causing prices to decrease. Elizabeth Clark, *Pricing the Last Mile*, NETWORK MAGAZINE, Feb. 1999, at 36.

[49] IDG News Service and Network World Staff, *A Day in the Life of the Internet*, NETWORK WORLD, Mar. 1, 1999, at 41, 44 (quoting Andy Schmidt, product manager for Ameritech's NAP service).

[50] E-mail from Stan Foster, Compaq Computer Corporation Mail and GroupWare Consultant, to Jeff Dunkelberger, Compaq Computer Corporation Senior Consultant (Feb. 8, 1999) (on file with author). Most large companies use one of the major telecomm companies as their sole ISP rather than go through the smaller ISPs. For example, Wrangler Corporation connected its Internet site directly to the Internet through the T1 telephone line connected to the major telecomm provider, Digex. Hanna Hurley, *Wrangler.com's Business Model: Behind the Pretty Face*, NETWORK MAGAZINE, Aug. 1998, at 38, 43.

[51] *Id.* A firewall is a system designed to prevent unauthorized Internet users from accessing private networks, such as Intranets, that are connected to the Internet. ZDNet, *ZDNet Webopaedia* (visited Oct. 20, 1999) <http://www.zdwebopedia.com/TERM/f/firewall.html>.

is little incentive to buy from smaller ISPs when Compaq can connect into the major telecommunications company.[52]

Corporations with direct connections similar to Compaqs' system[53] are the companies that clearly appear to be ISPs because they have instituted their own direct connections to the Internet and bypassed the smaller ISP.[54] Indeed, these companies follow the same process as a smaller ISP: they acquire web server and e-mail software, install it on the corporation's existing network, and buy the "wire" (the physical connection to the Internet) from the larger ISP, the major telecommunication company.[55] By following this relatively simple process, the corporation circumvents the smaller ISP and functions as its own ISP.[56] However, while the corporation may function as an ISP, it is not at all clear whether it has legal liability as an ISP.

Although the functional approach to ISPs was embraced in *Bohach v. City of Reno*, in which a city that owned and operated its own paging system was labeled an ISP,[57] Congressional attempts at defining Internet

---

[52] E-mail from Stan Foster, Compaq Computer Corporation Mail and GroupWare Consultant, to Jeff Dunkelberger, Compaq Computer Corporation Senior Consultant (Feb. 8, 1999) (on file with author).

[53] The following corporations are recognized as having direct Internet connections: the Joint Staff Pentagon, the Chief of Naval Operations Pentagon, the Bureau of Naval personnel, Learning Tree, BS/Warburg Dillon Reed, Fermilab, Brookhaven Lab, Eaton, Eli Lily, Harley Davidson, Tribune Broadcasting, ACNielsen, Sears Roebuck, Chicago Board of Trade, McDonalds and State Farm Insurance. E-mail from John Strider, Compaq Computer Corporation Senior Consultant, to Caitlin Garvey (Oct. 27, 1999) (on file with author); E-mail from John Featherly, Compaq Computer Corporation Solution Architect, to Caitlin Garvey (Oct. 27, 1999) (on file with author).

[54] Levitt & Comiskey, *supra* note 46. These companies decided it was cheaper and more efficient to manage these services internally, rather than outsource them to a third party. Levitt, *supra* note 46. In addition, many of these companies also noted security and cost concerns as reasons for becoming their own ISP. Levitt, *supra* note 46.

[55] E-mail from Stan Foster, Compaq Computer Corporation Mail and GroupWare Consultant, to Jeff Dunkelberger, Compaq Computer Corporation Senior Consultant (Feb. 8, 1999) (on file with author); UUNet, *Connection Guide* (visited Jan. 11, 2000) <http://www.uunet.com.html>.

[56] Paul McNamara, *Metering Messages*, NETWORK WORLD, Mar. 1, 1999, at 49. Bolstering the argument that these corporations are ISPs are reports that corporations with these systems are acting more like a traditional ISP by implementing charge-back policies to ensure that employees pay their fair share for any personal use. *Id.* "According to a survey of 50 organizations by Ferris Research of San Francisco, about 40% have implemented some kind of chargeback mechanism. Of that group, 22% assess charges based on overall network services, while just 18% are charging for e-mail usage only." *Id.*

[57] 932 F. Supp. 1232, 1236 (D. Nev. 1996). The court stated:

> The City is the "provider" of the "electronic communications service" at issue here: the Reno Police Department's terminals, computer and software, and the pagers it issues to its personnel, are, after all, what provide those users with "the ability to send or receive" electronic communications. But § 2701(c)(1) [of the Electronic Communications Privacy Act] allows service providers to do as they wish when it comes to accessing

providers have resulted in numerous statutory terms that do not clearly address the issue.[58] Although the statutory definitions are confusing, close study of the CDA and the DMCA indicates that Congress has embraced the functional, all-encompassing definition used by the technology industry. Under this functional definition, corporations with direct Internet connections, and arguably, even corporations that only purchase some services from other ISPs, are ISPs because they provide Internet access and services to their employees. The CDA[59] and the DMCA[60] demonstrate Congress' functional, pragmatic approach to ISPs, as the definitions of these statutes emphasize the broad nature of providers and the appropriateness of referring to corporations with direct Internet connections as ISPs.

1. The CDA's ISP Definition

The CDA uses the term "interactive computer service"[61] to refer to what the computer industry calls ISPs and defines them as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[62] Companies with direct Internet connections provide or enable computer access by multiple users to a computer server, including a system that provides access to the Internet. The CDA's broad definition emphasizes its inclusion of systems provided by educational institutions, which is the model of Internet connectivity followed by companies with direct Internet connections. Therefore, the CDA's definition appears to include corporations with direct Internet connections.

---

communications in electronic storage. Because the City is the provider of the "service," neither it nor its employees can be liable under § 2701.

Id.

[58] *See supra* notes 24-34 and accompanying text.

[59] 47 U.S.C. § 230 (1998).

[60] 17 U.S.C. § 512 (1998).

[61] The use of this term, rather than the term ISP, demonstrates the confusion surrounding Internet terminology. *See supra* notes 24-34 and accompanying text.

[62] 47 U.S.C. § 230(f)(2) (1998).

2. The DMCA's ISP Definition

The DMCA uses the term "service providers" to define "an entity offering the transmission, routing, or providing of connections for digital online 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."[63] Under this definition, corporations that offer the transmission or provide connections for online communications to their employees (and non-employees if the Intranet is connected to the Internet) of material of the employee's choosing, without modification to the material's content, are service providers.[64] Thus, corporations with direct Internet connections are providers under the DMCA's definition.

From a functionality perspective, the CDA's and the DMCA's reference to these corporation as ISPs makes sense because they are providing many, if not all, of the services that the smaller ISPs provide.[65] In addition, the rapid pace of technological development precludes a precise ISP definition which would become continually outdated and in need of amendment.[66] Instead, Congress appears to use broad definitions, albeit under various non-ISP labels, to simplify the technological issues.[67] Congress seems to have essentially embraced the industry's method of defining the Internet broadly, although forgoing the industry's use of the term "ISP" as the label for the broad definition. Therefore, the term ISP will be used throughout this Comment to refer to the broad, functional approach Congress and the industry take to service providers.

---

[63] 17 U.S.C. § 512(k)(1)(A) (1998).

[64] *Id.*

[65] *See supra* notes 42-60 and accompanying text.

[66] Indeed, the lack of recognition for corporations as ISPs appears to be primarily caused by the speed at which these corporations have embraced Internet technology. *See* Sheridan, *supra* note 1, at 166. Non-legal definitions of ISPs aptly illustrate how the rapid technological development has outpaced definitions, as non-legal definitions of ISP often reflect the tradition of paying the ISP to provide Internet services by making payment a component of the ISP definition. ZDNet, *ZDNet Webopaedia* (visited Oct. 20, 1999) <http://www.zdwebopedia.com/TERM/I/ISP.html>. However, "payment" is merely a reflection of the traditional ISP process, rather than a significant part of the ISP's function. Not only does the corporate ISP offer the same services as the traditional, smaller ISP, but also the employer is actually more reminiscent of earliest ISPs, such as universities, who provided Internet services to their "employees" at no charge. Thus, the basic function of the provider is the same for both traditional ISPs and corporate ISPs.

[67] 143 CONG. REC. E1452 (daily ed. July 17, 1997) (statement of Rep. Coble).

B. *Potential Liability for Corporate ISPs*

Under Congress' function-oriented ISP definition, corporations appear to take on the ISP title by operating as an ISP. However, the statutory ambiguity caused by the differing titles and the limited nature of the applicable statutes raises difficulties for corporate ISPs, as evidenced in both the CDA and DMCA. The issue becomes critical because employee computer abuse can result in civil,[68] and perhaps criminal, litigation against both employee and employer.[69] Possible plaintiffs include the intended targets of the employee's conduct (employees, customers, third parties),[70] unintended targets (third parties who loaded a virus-infected program or who inadvertently saw a malicious communication), clients of the employer (whose confidential data or trade secrets were disclosed), and other employees of the company (who may have had confidential data reviewed by the employee).[71] Faced with no direct, applicable statute and ambiguity in the existing statutes,[72] corporate ISPs are forced to look to statutes such as the CDA and the DMCA to determine both potential liability and protections from that liability.

1. Employer ISP Liability Under the CDA

With separate provisions for employers and ISPs,[73] the CDA aptly illustrates the difficulty corporate ISPs face as they try to determine potential liability resulting from employee computer abuse. Responding to increased litigation involving defamation via computer,[74] the CDA[75] offers

---

[68] Civil liability poses a great risk to the employer-provider and possible civil claims include sexual harassment, discrimination, fraud, and trademark and copyright infringement, invasion of privacy, and negligence. Garrity & Casey, *supra* note 2, at 25, 27.

[69] Peter Brown, *Developing Corporate Internet, Intranet and E-Mail Policies*, 520 PLI/PAT 347, 359-60 (1998).

[70] For example, in 1995, Chevron Corporation agreed to a 2.2 million dollar settlement of sexual harassment claims filed by four women based in part on off-color jokes transmitted via e-mail. Stansky, *supra* note 4, at 58. Likewise, in *Harley v. McCoach*, an employee used offensive e-mail messages as one proof of her claims of sex and race discrimination against her employer. 928 F. Supp. 533, 540 (E.D. Pa. 1996).

[71] Garrity & Casey, *supra* note 2, at 27.

[72] *See supra* notes 24-34 and accompanying text.

[73] 47 U.S.C. §§ 223(c), (e)(4) (1999).

[74] Defamation involves false statements referring to the plaintiff published to one or more third parties causing damage to the plaintiff. Kathy S. Frank, *Cable Online Liability*, 509 PLI/PAT 773, 794 (1998); Garrity & Casey, *supra* note 2, at 23-24. For example, defamation was involved when a software producer in a contract dispute allegedly placed a defamatory notice regarding the opposing

protection to both employers and providers from defamation claims in certain situations.[76] The uniqueness of the CDA is that it offers employers a defense separate from its provisions for providers, thereby suggesting that, although the CDA's definition for providers[77] is broad enough to include employers who are also ISPs, Congress either did not foresee employers in the role of ISPs or wanted to offer all employers protection regardless of their status as ISPs.

First, the CDA protects employers:

> No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.[78]

This provision's difficulty lies in its ambiguity. Provision (A) seems clear, requiring the defamatory conduct to be within the scope of employment and then only prescribing liability if the employer has knowledge of the conduct and authorizes or ratifies the conduct.[79] The trouble exists in Provision (B) as employers become liable if the conduct is within the scope of employment and the employer "recklessly disregards" the conduct.[80] The term "recklessly disregards" is not defined in the statute. According to

---

party's company on its web page and posted allegedly defamatory e-mail messages to that company's customers. Edias Software Int'l v. Basis Int'l, 947 F. Supp. 413, 419-20 (D. Ariz. 1996).

[75] The CDA also contained provisions designed to respond to minors' access to Internet pornography. 47 U.S.C. § 223(a) (1998). In *Reno v. ACLU*, the United States Supreme Court struck down the provisions regarding access and transmission of pornography. 117 S. Ct. 2329, 2344-50 (1997). The Supreme Court did not address the provisions pertaining to providers or employers so these provisions appear to remain valid. *Id.* at 2350. On October 21, 1998, President Clinton signed into law CDA's "replacement," "The Child Online Protection Act" which imposes fines and/or imprisonment for anyone who is "engaged in the business of selling or transferring material by means of the World Wide Web" and who fails to restrict access to "material that is harmful to minors." 1998 H.R. 4328, §§ 1401-1406 (West 1998);105 P.L. 277; 105 Enacted H.R. 4328.

[76] The protection for ISPs is not completely popular:

> By what rationale can the on-line companies be held liable? An appropriate analogy is the federal drug laws. Anyone who facilitates the commission of a drug offense in any regard is held to be equally guilty of the offense. The on-line companies are facilitating this material, and I believe that the same theory should apply to them; they should be held liable in order to resolve this problem.

Paul J. McGeady, *The Communications Decency Act of 1996: Keeping On-Line Providers On the Hook*, 11 ST. JOHN'S J. LEGAL COMMENT 733, 737 (1996) (internal citations omitted).

[77] *See supra* note 31 and accompanying text.

[78] 47 U.S.C. § 223(e)(4) (1998).

[79] *Id.* § 223(e)(4)(a).

[80] *Id.* § 223(e)(4)(b).

Webster's New World Dictionary, "disregard" means "to pay little or no attention to."[81]

The pairing of the term "recklessly" with "disregard" presents the greatest difficulty. With the inclusion of "reckless," the statute seems to establish a liability standard above mere negligence. Thus, the objective, reasonable person standard is not applicable because failure to do what a reasonable employer would normally do is negligent but not reckless. Therefore, the question becomes: what does an employer have to do in order to "recklessly disregard" an employee's computer abuse? Perhaps this imposes a "know or should have known" common law standard on the employer, or perhaps, a duty on the employer to pay some attention (although how much attention is the crux of this statute's ambiguity) to employees' acts through an "acceptable use" computer policy or monitoring program. Are employers liable for recklessly disregarding if they do not have "acceptable use" policies? Alternatively, does "reckless disregard" occur if the employer does not act after the employer knew or should have known about the misconduct? The statute simply does not say, and employers have an affirmative defense that they cannot completely understand.[82] Although an employer might be able to resort to the common law standard, the lack of certainty in the statute makes this solution unappealing. Due to the statute's ambiguity, any employer wishing to trigger this affirmative defense would be wise to institute an "acceptable use" policy to ensure that the employer has not "recklessly disregarded" the employee's misconduct.

Second, the CDA protects ISPs from defamation claims by stating that providers are not to be considered "publishers" or "speakers."[83] With this determination, the CDA halts a long-standing debate on whether ISPs were publishers, distributors, or common carriers[84] and, in so doing, freed ISPs

---

[81] 1121 (3rd College ed. 1988).

[82] Commentators discussing the CDA have also failed to address this issue and merely refer to this provision as a defense for employers. Anthony L. Clapes, *The Wages of Sin: Pornography and Internet Providers*, 13 No. 7 THE COMPUTER LAWYER 1 (1996); Adam S. Kirschner, *Highlights of the Telecommunications Act of 1996*, 183 Apr N.J. LAW. 29 (1997), James E. Meadows, *The Telecommunications Act of 1996: Rules of the Road for the New Highways*, 13 No. 3 THE COMPUTER LAWYER 1 (1996).

[83] 47 U.S.C. § 230(c)(1) (1999) (stating that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider").

[84] Frank, *supra* note 74, at 795. Publishers are deemed to have acquired knowledge of content of third parties through the process of editing and producing the publication and are treated as having adopted third-party content as their own and are liable for republication of the content. Distributors merely deliver or transmit content published by a third party and are generally not liable for defamatory content unless the distributor knows or has reason to know of the defamatory content. Common carriers are immune from liability for content of messages carried by their equipment. *Id.*

from the highest level of liability for defamation. For employers, this provision protects from liability for defamation by employees to third parties both outside and inside the corporation. Congress, through the CDA, urged providers to control Internet content by exempting providers from civil liability when they took voluntary, good faith actions to restrict access to or the availability of "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" material "whether or not such material is constitutionally protected."[85]

The first major case to test the CDA's provision was *Zeran v. America Online, Inc.*,[86] which concerned offensive messages posted on America Online ("AOL") that AOL failed to remove.[87] The court dismissed this claim, stating that it was precluded under the immunity provisions of the CDA.[88] The appellate court affirmed the ruling, further stating that Congress wanted to "encourage service providers to self-regulate the dissemination of offensive material over their services,"[89] which is why Congress immunized ISPs from forms of liability that discourage those providers from acquiring information about and control over the content on their systems.[90] Thus, the court recognized Congress' dual goals of promoting Internet technology and desiring decency in Internet content, but indicated that the desire to promote Internet technology was the prevalent goal:

> Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium . . . .
>
> . . . .
>
> . . . Interactive computer services have millions of users. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service

---

[85] 47 U.S.C. § 230(c)(2) (1998). This provision was expressly designed to overrule the holding in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, in which the New York Superior Court ruled that Prodigy could be liable as an ISP for defamatory statements made in a discussion area because Prodigy had tried to monitor the content of some of its on-line discussions. 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 25, 1995).

[86] 958 F. Supp. 1124 (E.D. Va. 1997).

[87] The messages regarded the bombing of the Murrah Federal Building in Oklahoma City and provided a telephone number to call "Ken" at the plaintiff's telephone number. *Id.* at 1126. Zeran had nothing to do with the messages and told AOL that the posting was false, but AOL failed to remove the posts. *Id.*

[88] *Id.* at 1135.

[89] Zeran v. America Online Inc., 129 F.3d 327, 331 (4th Cir. 1997).

[90] *Id.*

> providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.[91]

The next case to address ISP liability for defamation, *Blumenthal v. Drudge*,[92] raised the question of an ISP's level of control and its impact on potential liability.[93] To try to avoid CDA's immunity for ISPs, the plaintiffs argued that the business relationship between AOL and its online commentator, Matt Drudge, made AOL more active than a conventional ISP and, thus, rendered the CDA inapplicable.[94] This argument is analogous for a corporate ISP whose employee acts in a defamatory manner because the corporation is arguably more actively involved with the employee than a traditional ISP is with a subscriber. Although the judge agreed that fairness indicated that AOL's level of control suggested that liability was appropriate, he nonetheless found AOL not liable:[95]

> Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others. In some sort of tacit *quid pro quo* arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.[96]

Thus, the CDA currently grants ISPs a high level of immunity from defamation claims without requiring that ISPs control subscribers' Internet

---

[91] *Id.* at 330-31.

[92] 992 F. Supp. 44 (D.C. Cir. 1998).

[93] *Id.* This lawsuit by presidential advisor Sidney Bleumenthal and his wife against AOL regarded AOL "columnist" Matt Drudge's statement that Blumenthal had a "spousal abuse" problem. *Id.* at 44-48. The Blumenthals sued Drudge and AOL for libel, defamation, false light invasion of privacy, intentional infliction of emotional distress and slander. *Id.* AOL was accused of displaying a "reckless disregard" for the truth in knowingly distributing the unverified Drudge Report and not acting swiftly enough in removing the item. *Id.*

[94] *Id.* at 51-53.

[95] *Id.* at 51-52. This level of control debate raises the distinction between publisher and distributor liability, but the *Blumenthal* court stated, "Any attempt to distinguish between 'publisher' liability and notice-based 'distributor' liability and to argue that § 230 [of the CDA] was only intended to immunize the former would be unavailing. Congress made no distinction between publishers and distributors in providing immunity from liability." *Id.* at 52.

[96] *Id.*

content.[97] Furthermore, the CDA offers ISPs immunity for any action taken voluntarily and in good faith to restrict access to questionable material, but requires no action of the sort from ISPs in return for immunity.[98]

The CDA's provisions highlight the dilemma of corporate ISPs. None of the CDA's immunity provisions specifically address these corporations, and as a result it is unclear which provision is applicable. At first, it might seem that these corporations would seek to fall under the CDA's "employer" provision. Liability seems difficult to prove because the employee's actions must be in the scope of employment, and even if the actions are in the scope of employment, the employer must either have knowledge and ratify the conduct or recklessly disregard the conduct.[99] However, the ambiguity of the phrase "recklessly disregard" is troubling, as employers are left unsure of the requirements to achieve statutory immunity.

Furthermore, CDA's "provider" provisions seem to offer greater protection for employers who are ISPs because the provisions do not condition immunity on knowledge or reckless disregard of an employee's conduct and do not limit immunity to acts outside the scope of employment.[100] Likewise, the ISP provisions have been broadly interpreted in the *Zeran* and *Blumenthal* rulings, and the *Blumenthal* ruling clearly shows that the employer's level of control over the employee does not impact the immunity.[101] However, the lack of reference to corporate ISPs in this provision, and the separate provision for employers, raises the troubling question of whether Congress intended to consider corporations with direct Internet connections as something other than ISPs. No express answer exists, and the legislative history is silent, although it is probable that Congress did not even consider the likelihood that many corporations would have direct Internet connections during the provision's formation.

The dual provisions aptly illustrate the dilemma of corporate ISPs. Although the corporation's ISP status offers greater freedom and immunity from liability under the ISP provisions, attaining that freedom is difficult due to the requirements of the employer provision. Indeed, the employer provision's requirement that the employer must not have "recklessly disregarded" seems directly at odds with the *Blumenthal* court's ruling that

---

[97] 47 U.S.C. § 230(c)(2) (1998).

[98] *Id.*

[99] *Id.* § 223(e)(4).

[100] *Id.* § 230(c)(2).

[101] 992 F. Supp. 44 (D.C. Cir. 1998).

the ISP was under no obligation to control the defamatory content.[102] Despite the allure of the ISP provisions, corporate ISPs would be wise to avoid complete reliance on either provision, due to the employer provision's ambiguity and the discrepancies between the employer and ISP provisions. Instead, corporate ISPs should combine the two provisions and exert some sort of control over Internet content with an "acceptable use" computer policy to meet the employer provision[103] while claiming the greater immunity offered through the ISP provision. Hence, corporate ISPs should: 1) implement an "acceptable use" computer policy and a monitoring program, thereby minimizing or eliminating a claim of "reckless disregard" for employee conduct under CDA's employer provision; and 2) claim the protection CDA offers to ISPs because the ISP immunity is not limited by scope of employment, as is the employer provision, but covers all subscriber activity. Therefore, the CDA emphasizes the dilemma facing corporate ISPs and offers no clear guidance for corporate ISPs beyond some indications of methods to possibly attain immunity and limit potential liability.

2. Employer ISP Liability and the DMCA

The DMCA provides limitations on liability for copyright infringement by ISPs in certain circumstances, such as system caching[104] and transmissions initiated by a third party.[105] Transferring files through the World Wide Web, file attachments, or "cut and paste" in e-mail messages is a common use for systems accessing the Internet.[106] Legal issues arise when these transfers contain copyrighted material, and the danger for companies is that employees will either publish copyrighted corporate information onto the Internet or incorporate copyrighted non-corporate works into a company product.

---

[102] *Id.*

[103] Although the CDA's requirements for employer's monitoring of employee Internet content are unclear, the *Zeran* court specifically addresses Congress' desire for some sort of control over content. Zeran v. America Online, Inc.,129 F.3d 327, 330-31 (4th Cir. 1997). Furthermore, even if Congress is unwilling to place that burden on a traditional ISP, Congress would seem to have no such qualms about placing that burden on employers who are also ISPs because the employers' status allows monitoring, and the corporate need for Internet technology would not permit a decline in Internet growth, despite monitoring requirements.

[104] A system cache is a temporary storage mechanism. ZDNet, *ZDNet Webopaedia* (visited Oct. 20, 1999) <http://www.zdwebopedia.com/TERM/c/cache.html>.

[105] 17 U.S.C. § 512 (1998).

[106] HILLS, *supra* note 14, at 26-28.

The DMCA's immunity provisions accentuate the differing level of control between corporate ISPs and traditional ISPs, because corporate ISPs' position as employer allows them to control users' content,[107] as long as privacy concerns grounded in common law,[108] state statutes,[109] and the ECPA[110] are considered. In an effort to increase Internet technology by not discouraging ISPs with increased potential liability, the DMCA offers immunity to those ISPs who presumably have the least ability to prevent liability due to their low level of control over users.[111] Thus, because most traditional ISPs have little intrinsic control over their users, they receive extensive immunity.[112] However, corporate ISPs' innate control over their users by virtue of the employment relationship limits their immunity.[113] The DMCA emphasizes this difference in ISP immunity, as provision (A) seems to apply to traditional ISPs, and provision (B) appears to apply to corporate ISPs:

> (1) In general. A service provider shall not be liable for monetary relief, . . . for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider –

---

[107] Lee, *supra* note 5, at 155.

[108] The common law right of privacy encompasses four distinct causes of action: 1) misappropriation of the plaintiff's name or likeness without her consent; 2) intrusion by the defendant into an area in which plaintiff's reasonable expectations of privacy are violated; 3) public disclosure of private facts about the plaintiff; and 4) portrayal of the plaintiff in a false light in the public eye. RESTATMENT (SECOND) OF TORTS § 652(A) (1977). In an intrusion claim rising from computer monitoring, an employee will claim that the employer violated her reasonable expectation of privacy, concentrating on the second cause of action listed above. To avoid this issue if monitoring is desired, an employer must lower the reasonable expectations of privacy in the workplace by posting signs, addressing the issue during training, and having the employee sign a written notice.

[109] A state might have a statute detailing employee privacy rights, such as Article 250 of New York's Penal Law which prohibits intercepting or accessing electronic communications without at least one party's consent. N.Y. PENAL LAW § 250 (McKinney 1998).

[110] 18 U.S.C. § 2511(2)(b) (1998). Employers desiring to monitor e-mail must consider the ECPA, which protects employees of certain employers from monitoring in particular situations. If ECPA applies and the employer wants to monitor employee computer use, the employer should attain a consent form to fit into the ECPA's consent exception. *See supra* note 5 and accompanying text.

[111] 17 U.S.C. § 512(c) (1999). Congress' focus on level of control as the determinant for ISP immunity was evident in the On-Line Copyright Liability Limitation Act, the precursor to the DMCA: "The availability of the exemption depends on the actor's level of control, participation, and knowledge of the infringement, rather than on the particular type of technology used or the particular type of business being conducted." 143 CONG. REC. E1452 (daily ed. July 17, 1997) (statement of Rep. Coble).

[112] Sarah Whalley, *Comparing Approaches to ISP Liability*, 5 No. 3 MULTIMEDIA STRATEGIST 1, 1-3 (1998).

[113] 17 U.S.C. § 512 (1999).

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.[114]

Provision (A) appears to apply to the traditional ISP who does not generally have the ability or right to monitor subscriber's usage and, thus, is not liable unless the ISP had knowledge and failed to act upon that knowledge.[115] Provision (A) allows an ISP to escape liability unless the ISP had knowledge and failed to act on that knowledge.[116] This high threshold protects the ISP from most cases of direct[117] or contributory[118] copyright infringement by promoting the ISP as a passive entity lacking the necessary control to fairly impose liability. This immunity reflects Congress' desire to promote technological growth by not placing high demands on traditional ISPs to monitor subscribers' computer use[119]

---

[114] *Id.* §§ 512(c)(1)(A), (B).

[115] *Id.* § 512(c)(1)(A).

[116] *Id.*

[117] The elements of direct infringement include: 1) ownership of a valid copyright and 2) violation of the plaintiff's exclusive rights by the defendant. Frank, *supra* note 74, at 783. Direct infringement does not often arise for ISPs because the ISP must actively participate in the infringement to be liable. Daniel R. Cahoy, Comment, *New Legislation Regarding On-Line Service Provider Liability For Copyright Infringement: A Solution in Search of a Problem?* 38 IDEA, 335, 360 (1998); *see also* Marobie-Fl, Inc. v. National Assoc. of Fire Equipment Distrib. and Northwest Nexus, Inc., 983 F. Supp. 1167 (N.D. Ill. 1997) (holding that an ISP was not liable for direct infringement because the ISP offered only the means to copy, distribute, or display plaintiff's works, much like the owner of a public copying machine who did not engage in the activities but was merely used by a third party to copy protected material); Playboy Enters. Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (holding that a bulletin board operator was liable for direct copyright infringement for providing copies of Playboy photographs for subscribers).

[118] Contributory liability may be found only when "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another." Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (internal citations omitted); *see also* Sega Enters. Ltd. v. Maphia, 948 F. Supp. 923 (N.D. Cal. 1996) (holding that a bulletin board operator who encouraged subscribers to upload and download unauthorized copies of Sega's video games liable for contributory infringement).

[119] S. REP. NO. 99-541, at 5 (1986) (stating that legal uncertainty over the privacy status of new forms of communication "may unnecessarily discourage potential customers from using innovative communications systems").

because the ISPs do not have to act as long as they have no knowledge of computer misuse.[120]

Provision (B) differs extensively from provision (A) and appears to target corporate ISPs with its application to service providers who have the "right and ability to control such [infringing] activity."[121] Corporations with direct Internet connections first meet DMCA's criteria for service providers because they are an "entity offering the transmission, routing, or providing of connections for digital online 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."[122] Second, corporate ISPs have the "right and ability" to control their users' activity through their position as employer and the exceptions in the ECPA that allow monitoring of certain content. Thus, Provision (B) appears to speak directly to corporate ISPs.

Provision (B) awards ISPs immunity only if they do not financially benefit from the infringing activity, an immunity much more limited than the sweeping immunity given traditional ISPs in provision (A).[123] Under provision (B), a corporate ISP cannot use its ISP status to acquire immunity for computer abuse that benefits the company, such as copyright infringement done for company publications. Rather, that corporation is liable for any copyright infringement via the Internet if the corporation financially benefits from the infringement.[124]

Immunity is only achieved through absence of financial benefit. Because unsuspecting employees working on company projects can easily infringe copyrights, the DMCA offers corporate ISPs further motivation to implement "acceptable use" policies and to monitor computer use in order to avoid innocent infringements done for the company's financial benefit. Since immunity is only lost for receiving a financial benefit from the infringing activity, the ease of innocent copyright infringement for the corporation's financial benefit creates a strong incentive to control content.[125]

---

[120] 17 U.S.C. § 512(c)(1)(A) (1999).

[121] *Id.* § 512(c)(1)(B).

[122] *Id.* § 512(k)(1)(A)(a).

[123] Provision (B) provides immunity for vicarious copyright infringement. *Id.* § 512(B). To prove vicarious liability, a plaintiff must show that the third party: 1) had the right and ability to control the primary infringer and 2) received a direct financial benefit from the infringement. Frank, *supra* note 74, at 783; Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304 (2d Cir. 1963).

[124] Cahoy, *supra* note 117, at 360.

[125] *Id.*

The DMCA emphasizes the negligence standard of liability on ISPs.[126] For traditional ISPs, the less an ISP acts in a reasonably prudent manner in addressing claimed infringement, the more likely the ISP will be held liable.[127] Immunity for traditional ISPs is not conditioned on their ability to control a user's computer use and demonstrates that no duty is imposed on the traditional ISP until a claimed infringement exists.[128] Corporate ISPs face a much higher standard, as emphasized in the separation of corporate ISPs from traditional ISPs, by the corporation's right and ability to control employee computer use.[129] The absence of any immunity if the corporation financially benefits from the infringement further emphasizes the heightened duty for corporate ISPs because it effectively places an unspoken duty of controlling content on the corporation.[130] Indeed, this provision indicates that corporate ISPs might have to do more than simply institute "acceptable use" policies, but actually monitor content to avoid liability since no immunity is provided for good faith effort, only for results. Therefore, corporate ISPs should institute both "acceptable use" computer policies and monitoring programs to protect themselves from liability under the DMCA.

C. Methods by which Corporate ISPs Can Minimize Liability

Corporations with direct Internet connections should institute "acceptable use" computer policies and monitoring programs to limit potential liability.[131] While a policy limited to e-mail used to be sufficient to curb liability, current technology makes a limited policy impractical and

---

[126] Jose I. Rojas, *Liability of ISPs, Content Providers and End-Users On the Internet*, 507 PLI/PAT 1009, 1034-35 (1998).

[127] *Id.*; 17 U.S.C. § 512 (A) (1999).

[128] 17 U.S.C. § 512 (A) (1999).

[129] *Id.* § 512 (B).

[130] *Id.*

[131] Kevin J. Baum, Comment, *E-Mail In the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1035-40 (1997). Because the concept of corporate ISPs is relatively recent, most corporations with existing acceptable use policies instituted them to avoid liability for common employment law claims, such as sexual harassment, since the policy assists in proving a commitment to a non-hostile work environment. *Id.* "The bottom line is most large companies provide their own [I]nternet connection to reduce cost. Of course, they absorb the risks associated with this access . . . . Risk can be lessened with software solution[s] such as dirty word checkers to check against content, and IP blockers to prevent trips to questionable sites." E-mail from John Strider, Compaq Computer Corporation Senior Consultant, to Caitlin Garvey (Oct. 27, 1999) (on file with author).

unwise.[132] However, it is difficult to determine how extensive a corporation must be in its fight against computer abuse. The unsettled nature of this area complicates determining whether employers must actually monitor content or simply institute "acceptable use" policies. In addition, employers must determine whether they should control all computer Internet content or if controlling e-mail is sufficient.[133] Although the DMCA appears to indicate that monitoring is required to avoid liability,[134] the CDA's use of the ambiguous phrase "recklessly disregard" provides no insight into the matter. To be safe, corporate ISPs seeking protection from liability should implement: 1) an "acceptable use" computer policy that covers all the corporate computer system's applications and 2) a monitoring program to effectuate the policy.[135]

1. Institute "Acceptable Use" Computer Policies[136]

An effective "acceptable use" computer policy establishes the corporation's official position on employee computer usage and provides grounds for disciplinary action for policy violation.[137] Despite the potential

---

[132] *See supra* notes 2-5 and accompanying text. Computer abuse can also occur via chat rooms, newsgroups, or the World Wide Web; therefore a policy limited to e-mail does not adequately address the potential situations for computer abuse. *Id.*

[133] These issues are beyond the scope of this Comment, as the ambiguity of this area of law makes the initial questions of 1) whether corporations with direct Internet connections are indeed ISPs, and 2) if so, what level of immunity do they receive, more immediate.

[134] 17 U.S.C. § 512(c)(1) (1999).

[135] Michael D. Scott, *Creating A Corporate Internet Acceptable Use Policy*, LEGAL WORKS '98, at 3. Although the law is unsettled as to whether an acceptable use computer policy is sufficient to attain immunity for computer abuse, monitoring programs of some sort appear required. *Id.* For an acceptable use computer policy to have any genuine significance, a corporation must exert a reasonable effort to determine whether the policy is followed. *Id.* Furthermore, if the employer states that it has the right to monitor communications and makes no effort to do so, its corporate policy will do little to limit the employer's liability for improper communications. *Id.*

[136] This section offers guidance on "acceptable use" policies, which should comprise merely one part of a corporate computer usage policy. For a thorough source on computer usage policies, see A GUIDE TO DEVELOPING COMPUTING POLICY DOCUMENTS, SHORT TOPICS IN SYSTEM ADMINISTRATION 2 (Barbara L. Dijker, ed. USENIX Association for SAGE, the System Administrators Guild, 1996).

[137] Diana J.P. McKenzie, *Information Technology Policies: Practical Protection in Cyberspace*, 3 STAN. J.L., BUS. & FIN. 84, 84 (1997). As a matter of good practice, cross-references to the company's existing sexual harassment and discrimination policies should be provided in the policy. *Id.* In addition, employees should sign acknowledgement forms that they read and understood the policy and consent to the policy's terms. *Id.* The acknowledgement form complies with the ECPA's consent exception. *Id.*; 18 U.S.C. § 2511(2)(b) (1999). Because this area of law is unsettled, corporate ISPs would be wise to follow the ECPA's requirements for monitoring despite the CDA and DMCA's provisions that seem to expect employer monitoring but do not mention ECPA's limitations. The policy should be re-circulated at training sessions (with another acknowledgement form) to remind employees of the need for compliance. Brown, *supra* note 69, at 368-69.

liability for computer abuse, many corporations avoid instituting "acceptable use" computer policies.[138] Absence of an "acceptable use" computer policy is disturbing when compared to the potential for employee computer abuse and the insight gleaned from applicable statutory provisions. Despite the statutes' ambiguities, Congress' desire for control of Internet content by entities that have the ability to control content is clear.[139] Thus, corporations should institute these policies as both preventative measures and protection from liability. While no complete safeguard to avoiding liability exists due to the unsettled nature of this area, "acceptable use" computer policies seem to be the minimal requirements for avoiding liability.

An effective "acceptable use" computer policy should initially address general privacy issues to lower any reasonable expectations of privacy the employee might have in accordance with ECPA.[140] For example, the policy should state that: the corporate computer system, including e-mail and software, is company property that should only be used for company purposes;[141] employees do not have a personal privacy right in anything created, received or sent from the corporate computer system;[142] the corporation has the right to monitor employee computer use; and passwords and user IDs do not limit corporate monitoring of an employee's account.[143]

---

[138] This avoidance of acceptable use policies is illustrated in a recent study that found that most corporations had no restrictions or only general restrictions on non-business related activity during working hours. Levitt, *supra* note 49, at Table 9 (noting that 60 out of 172 companies responding to a survey stated that they have no restrictions imposed on employee use of the Internet). Likewise, the Corporate Information Technology "*Policies and Procedures Survey of Internet Use and Polices*" showed that of those companies responding, ninety-eight percent allowed Internet access to some of their employees, but almost two in five companies did not have a formal "acceptable use" policy and many policies did not address significant issues such as business versus personal use of the Internet and the types of information that can be accessed or downloaded. McKenzie, *supra* note 137, at 84.

[139] Zeran v. America Online, Inc., 129 F.3d 327, 330-31 (4th Cir. 1997).

[140] 18 U.S.C. § 2511 (1998).

[141] Brown, *supra*, note 69 at 368-69; Vincent I. Polley, *A Model Electronic Communications Policy for the Workplace*, 44 No. 7 PRAC. LAW 25 (1998); McKenzie, *supra* note 137; Michael D. Scott, *Creating a Corporate Internet Acceptable Use Policy*, GLASSER LEGAL WORKS 75 (1988); Julienne W. Bramesco, *Employee Privacy: Avoiding Liability in the Electronic Age*, 562 PLI/LIT 515, 529-30 (1997).

[142] Frank C. Morris, *Issues From the Electronic Workplace E-Mail Communications: The Developing Employment Law Nightmare*, SB07 ALI-ABA 335, 349-50 (1996).

[143] Brown, *supra* note 69, at 368-69. Likewise, the policy should address general issues such as: any communications online that would be illegal if communicated orally or in written form are prohibited; derogatory, obscene, defamatory, and harassing communications are prohibited; solicitations or proselytizing for charitable, religious, political or other non-business purposes are prohibited. *Id.*

To protect corporate security,[144] the policy should detail that: all Internet access between corporate networks and public networks must occur through a corporate firewall; corporate-approved and supported software must be used to access the Internet; files obtained from any outside source must be scanned for viruses, including Internet file transfer and e-mail attachments; and highly sensitive data sent over the Internet must be encrypted.[145]

In an effort to receive DMCA's immunity, the policy should also address copyright issues and inform employees that: the transmission of trade secrets, confidential communications, or privileged communications over the Internet is prohibited;[146] the unauthorized copying and distribution of copyrighted materials is prohibited; copyrighted or patented materials must contain proper copyright and patent numbers before being placed on the computer system; and transferring, downloading, or otherwise duplicating copyrighted materials without permission of the copyright owners is prohibited.[147]

The policy should also address e-mail, newsgroups, chat rooms, and the World Wide Web in an effort to decrease potential liability for defamation, harassment, and discrimination. Regarding e-mail, chat and newsgroups, the policy should communicate that: these services should be primarily used for business purposes, with personal use limited to a minimum (or excluded altogether);[148] chain letters, "top ten" lists, and other non-business-related mailing lists are prohibited; internal e-mail may not be distributed to anyone outside of the corporation unless the e-mail provides for public distribution; and deleted e-mail messages are not deleted off the computer system but are merely removed from the employee's computer.[149] Regarding the World Wide Web, the policy should inform employees to

---

[144] This section addresses broader issues than liability concerns, such as the risk that an employee will innocently or maliciously release corporate trade secrets or confidential information outside the corporation.

[145] Stephen W. Feingold, *E-Mail & Internet Update: An Employee's Perspective*, 6 EMPLOYMENT LAW STRATEGIST 1, 4 (July 1998). In addition, the policy should state that: images must not be saved to the cache of a network drive; address lists should not be posted or distributed outside the corporate Intranet without proper encryption; employees must protect their passwords by selecting passwords that include both alpha and numeric characters, change their passwords frequently, and refrain from disclosing them; and any files or documents from the Internet or received from outside e-mail must be scanned for viruses. Brown, *supra* note 69, at 368-69.

[146] Brown, *supra* note 69, at 363-64.

[147] *Id.* at 368-69.

[148] *Id.* at 368-69. Some policies that allow personal e-mail require all personal e-mail to include a disclaimer that the views expressed in the e-mail are personal views of the sender and do not reflect the views of the company. Feingold, *supra* note 145, at 4.

[149] Brown, *supra* note 69, at 368-69; Feingold, *supra* note 145, at 4.

avoid inappropriate Web sites and limit Web activity to corporate business.[150]

2. Institute Monitoring Programs

Although it is unclear if a corporate ISP must institute a monitoring program to attain immunity, some form of a monitoring program appears to be wise.[151] Indeed, if an employer adopts an "acceptable use" computer policy that provides for monitoring, the employer should actually implement the policy.[152] Failure to implement the policy could give rise to a claim that an employee's expectation of privacy was restored over time, which causes the employer's act of monitoring to violate the ECPA.[153]

Corporations who refrain from monitoring often feel that monitoring detracts from the employment relationship by instituting an element of distrust between employer and employee.[154] However, avoiding monitoring to maintain a positive employment environment may not be an effective or wise decision, since one in six respondents to the "*Corporate Information Technology Policies and Procedures Survey*" reported noticeable negative effects from employee Internet use, and, perhaps more importantly, Congress has not clearly indicated what level of control over content it demands in return for corporate ISP immunity.[155]

Although a monitoring program should be restricted to furthering the corporation's legitimate business objectives[156] and should be disclosed in

---

[150] The policy could also state that employees must not access or store inappropriate or offensive graphics, games or other materials on corporate computer systems and that Web surfing must not interfere with an employee's job function. Brown, *supra* note 69, at 368-69.

[151] Beverly W. Garofalo, *What Employers Need to Know to Protect Themselves*, 13 No. 12 COMPUTER LAW STRATEGIST 1, 5 (Apr. 1997); 18 U.S.C. § 2511 (1998).

[152] Garofalo, *supra* note 151, at 5.

[153] *Id.* at 5.

[154] Levitt, *supra* note 46. Other employers fear that the very act of monitoring employees' actions will cause the employer to be liable under agency law because agency law states that when extensive control is exercised by the principal over the agent, it is more likely that the principal will be responsible for the conduct and misconduct of the agent. Anne E. Lehman, *E-Mail In The Workplace: Question Of Privacy, Property Or Principle?*, 5 COMMLAW CONSPECTUS 99, 11-12 (1997); RESTATEMENT (SECOND) OF AGENCY § 140 (1958). Although technically correct, this argument fails when compared to statutes such as DMCA and CDA that clearly suggest that a head in the sand posture will not preclude liability for employee computer abuse. Instead, corporate ISPs appear expected to use their position as employer to control content.

[155] McKenzie, *supra* note 137.

[156] An employer should refrain from reviewing the content beyond determining that the content is not business-related. Brown, *supra* note 69, at 357.

the "acceptable use" policy,[157] a monitoring program can be passive or active through the use of blocking, filtering, or monitoring software.[158] First, blocking software is the most active type of monitoring program and generally relies on a precompiled database of sites that are categorized and blocked according to the content (or sometimes even a combination of letters) the maker of the software deems "inappropriate."[159]

Second, filtering software does not block whole sites or domains based upon their content, but rather by their category and address.[160] For example, Compaq does not allow its employees to access the category "weapons," which filters out the United States Olympic shooting team, non-profit firearms safety organizations, the United States government site for the Civilian Marksmanship Program, Remington and other related sites.[161] Thus, a major problem with blocking and filtering is that valuable corporate research might not be able to get past the block or filter.[162]

Third, monitoring software is the most passive of the monitoring programs by using access control software that simply denotes where an employee goes on the computer system.[163] This method is the most common and works well because each user has a unique number assigned to that user's account and that number is applied to a list that controls access to resources.[164] The monitoring software tracks each employee's Internet usage, including the sites the employee visits, the time the employee spends there, and e-mail the employee sends.[165] The weakness

---

[157] Lisa Macko, *Who's Reading Your E-Mail at Work?*, (visited Oct. 20, 1999) <http://www.zdnet.com/zdnn/stories/comment/0.5859.2256385,00.html>. Due to the uncertainty in this area of law, an employer would be wise to disclose its monitoring program in its "acceptable use" policy distributed to all employees. *Id.* This disclosure would limit employee claims regarding violation of employee privacy rights by essentially obtaining the employee's consent to the monitoring. *Id.*

[158] Stephanie Izarek, Net Watch (visited Jan. 23, 1999) <http://www.zdnet.com/computershopper/edit/cschopper/content9809/341927.html>.

[159] *Id.* For example, Kansmen Corporation's Little Brother 2.0 uses packet sniffing technology to track and block employee access to the Internet. Jim Rapoza, *Keeping a Sharper Eye on Internet Users*, (visited Oct. 20, 1999) <http://www.zdnet.com/pcweek/reviews/0223/23access.html>. Little Brother 2.0 allows employers to see the sites employees were accessing in real time. *Id.* Little Brother 2.0 pre-rates many sites into suitability categories, but also allows employers to re-rate those sites and to specifically block other sites. *Id.* An employer can also block sites whose address contains specific words. *Id.*

[160] *Id.*

[161] Compaq Messaging Interest List, Feb. 10, 1999.

[162] Izarek, *supra* note 158.

[163] *Id.*

[164] *Id.*

[165] *Id.* In addition to addressing potential liability, monitoring programs are also used to keep corporate costs down. *Id.* A survey of fifty companies showed that forty percent have chargeback policies to dock employee pay for e-mail messages sent over a certain limit, in an effort to keep

with monitoring software is that the system is based strictly on trusting the user to not share the user ID or password with others, and that the user ID or password will not become compromised by other means, such as a computer hacker.[166] Thus, employer action should not be based solely on monitoring software, and employers must verify the identity of an alleged violator before acting.[167]

It is estimated that twenty-three percent of corporations currently connected to the Internet have installed some type of monitoring program.[168] As is indicated by the variety of software, the options are extensive for corporations instituting a monitoring program. The extent of the options, coupled with the legal ambiguities for corporate ISPs, indicate that although corporate ISPs should have some sort of monitoring program to limit potential liability, the intensity of the program depends on the corporation.

IV. CONCLUSION

Recent technological advances have thrust employers into uncharted legal waters. Although, neither the courts nor Congress have specifically addressed this issue, the functional approach of existing statutory definitions indicate that corporations with direct Internet connections are ISPs. Corporate ISPs do not, however, appear to automatically receive the immunity granted traditional ISPs. Instead, ISP immunity appears to be conditioned upon corporate ISPs' "level of control," which essentially requires corporate ISPs to control its users' computer content to attain immunity. Thus, corporate ISPs appear able to win immunity from liability, but only through effective "acceptable use" computer policies and monitoring programs. Although corporate ISPs' implementation of

---

personal usage of e-mail at a minimum and decrease the costs of messaging systems. Paul McNamara, *Metering Messages*, NETWORK WORLD, Mar. 1, 1999, at 49.

[166] Rosove, *supra* note 5. For example, if a user visits a pornographic site, the corporate audit logs will show that that the user's ID visited that site – not necessarily the user himself. Rather, a hacker could be accessing the site under the user's ID.

[167] Rosove, *supra* note 5.

[168] Troy Dreier, *Corporate Monitoring Tools* (visited Jan. 23, 1999) <http://www.zdnet.com/products/stories/reviews/0,4161/5-6/99>. According to a 1999 study by the American Management Association, twenty-seven percent of all employers already monitor employee e-mail randomly. Lisa Macko, *Who's Reading Your E-Mail at Work?*, (visited Oct. 20, 1999) <http://www.zdnet.com/zdnn/stories/comment/0.5859.2256385,00.html>.

policies and monitoring programs may disturb some commentators,[169] corporations can ill afford to ignore this area of potential liability and must institute the policies and programs to attain immunity until Congress clearly addresses this issue.

[169] Izarek, *supra* note 158. Stating "content hysteria has set in, and the very corporations that demanded administrators rush to get Net access are now asking them to curtail it in the new role of 'cyber cops.' This is classic 'protect us from ourselves' syndrome, and frankly, I don't like where it may lead." *Id.*