Boston University
Journal of Science & Technology Law

Comment

Computer Crimes and the Respondeat Superior Doctrine: Employers Beware

Mark Ishman

Table of Contents

Computer Crimes and the Respondeat Superior Doctrine: Employers Beware

Mark Ishman†

I. INTRODUCTION

1. Imagine that it is Friday afternoon and Mr. White, the manager of office services at ANGELIC Company, asks Bob, an employee whom he supervises, which National Football League ("NFL") stars he plans to select to start this week in his "fantasy football league."[1] Bob replies, "Brett Favre, Emmitt Smith, Jerry Rice, Shannon Sharpe and Morten Anderson."[2] Mr. White responds with encouragement, "Sounds like a winner to me." Shortly thereafter, Bob uses the company's computer to log[3] onto the "Internet"[4] to perform company business. During this Internet session,

† Mark W. Ishman is a law clerk at Baker & McKenzie in their Chicago office IT/C Practice Group. He is a candidate for his J.D./LL.M in information technology from the John Marshall Law School in January 2001. Among his publications: *Trends in U.S. Copyright Law: Adapting to the Cyberrevolution*, COMPUTER WORLD, Apr. 2000 (co-author); and *A Consumer's Analysis of the Electronic Currency System and the Legal Ramifications for a Transaction Gone Awry*, 6 MURDOCH UNIV. ELECTRONIC J.L. 3 (Sept. 1999) <http://www.murdoch.edu.au/elaw/issues/v6n3/ishman63_text.html> (co-author).

[1] Ten or twelve fans simulate that they are owners of an NFL football team. *See* Adam D. Thierer, *Don't Rain on my "Field of Dreams"* (last modified Apr. 17, 2000) <http://www.heritage.org/views/98/ed041798b.html>. Each fan chooses a team name. Collectively, they agree to a scoring system and "some basic ground rules" and have a hypothetical draft of real football players from the NFL. *Id.* Indubitably, each fantasy league member wagers money that his or her fantasy football team will outplay the other. *See id.*

[2] Brett Favre is the starting quarterback for the Green Bay Packers; Emmitt Smith is a starting running back for the Dallas Cowboys; Jerry Rice is the starting wide receiver for the San Francisco 49ers; Shannon Sharpe is the starting tight end for the Denver Broncos; and Morten Anderson is the starting place kicker for the Atlanta Falcons. *See generally* National Football League, *Teams* (last modified Apr. 21, 2000) <http://www.nfl.com/teams/>.

[3] An employee typically gains access to a company's computer system by entering a password. *See* C. Forbes Sargent, III, *Electronic Media and the Workplace: Confidentiality, Privacy and Other Issues*, 41 BOSTON B.J., May/June 1997, at 6, 6. Thereafter, the computer stores each and every step the user takes on the Internet, including Internet gambling activity and communications via e-mail. *See id.* Additionally, it is theoretically possible to retrieve even deleted e-mail. *See id.*

[4] The Internet is "a giant network which interconnects innumerable smaller groups of linked computer networks." ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996), *quoted in* Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456, 459 (E.D. Pa. 1996). As noted by numerous courts, the Internet is a unique, international, as well as interstate phenomenon. *See, e.g.*, Reno v. ACLU, 521 U.S. 844, 850 (1997); Lockheed Martin Corp. v. Network Solutions, Inc., 985 F.

Bob verifies that the mail that ANGELIC sent arrived at its destination by accessing the Federal Express Website. While at the Federal Express Website, Bob remembers that he must change his starting line-up for this weekend's games. Bob quickly interrupts his daily work, accesses his fantasy football Website and enters this week's starting line-up for his fantasy football team. After finalizing his starting line-up, Bob returns to the Federal Express Website and completes his daily work.

2. If Internet gambling is illegal in Bob's state, can ANGELIC Company be held liable for Bob's fantasy football league? ANGELIC Company had knowledge of Bob's activities, and Bob used the company's computer while engaged in the scope of his employment. Moreover, what if ANGELIC Company had a policy prohibiting all non-business and illegal Internet activity and had monitored Bob's activity on the Internet but failed to discipline him? Moreover, what types of sanctions could state and federal governments impose on ANGELIC Company for the illegal activity of Bob, its employee?

3. The purpose of this Comment is to explain an employer's potential liability exposure when an employee at its workplace conducts illegal online activity. Part II begins with a general discussion of technology in the workplace. Next, it focuses on traditional and modern theories of respondeat superior[5] and explains when an employer may be held liable for an employee's illegal activity. Part III follows with analysis regarding when an employer may be held liable when it allows its employees the right to use its equipment and they thereby conduct illegal online activity. Lastly, this Comment proposes several necessary precautions that all employers that utilize modern technology in the workplace must take to avoid liability.

II. BACKGROUND

4. Both technology in the workplace and computer crime laws have expanded enormously over the last ten years.[6] However, modern law has failed to keep up with

---

Supp. 949, 951 (C.D. Cal. 1997); American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 164 (S.D.N.Y. 1997); Hearst Corp. v. Goldberger, No. 96 Civ. 3620, 1997 WL 97097, at *1 (S.D.N.Y. Feb. 26, 1997); Shea *ex rel.* Am. Reporter v. Reno, 930 F. Supp. 916, 925 (S.D.N.Y. 1996); *see also* Sam Puathasnanon, *Cyberspace and Personal Jurisdiction: The Problem of Using Internet Contacts to Establish Minimum Contacts*, 31 LOY. L.A. L. REV. 691, 694 & nn.24-27 (1998) (discussing the development, operation and current use of the Internet).

[5] "Respondeat superior" is a Latin phrase meaning "let the superior make answer." BLACK'S LAW DICTIONARY 1313 (7th ed. 1999). In other words, the employer is liable in certain situations for the wrongful or illegal acts of its employee. *See id.*

[6] For commercial use, the Internet allows companies (both internally within the company and to its clients and the general public) to communicate and advertise, and allows the consumer to access its goods and services directly. *See Lockheed Martin Corp.*, 985 F. Supp. at 951; *see also* Louise Ann Fernandez, *Workplace Claims: Guiding Employers and Employees Safely Through the Revolving Door, in 26th Annual Institute on Employment Law*, at 775, 790 (PLI Litig. & Admin. Prac. Course Handbook Series No. H4-5272, Sept. 1997), *available in* WESTLAW, PLI/Lit File (explaining why the

technology in regulating illegal online activity.[7] Presently, both state and federal laws are being enacted to help halt this expansion by holding employers liable for the illegal online activity of its employees.[8] Thus, employers may be liable for their employees' illegal online activity.[9]

A. Technology In The Workplace

5. "The Internet is a giant network [that allows global communication between] people, institutions, corporations and governments."[10] Between 1983 and 1994, the Internet "underwent an explosive growth period with the number of host computers and users doubling every year. . . ."[11] Moreover, as of January 2000, there were approximately 248 million Internet users worldwide[12] and more than 70 million top-level domain names.[13] One of several reasons for the Internet's phenomenal growth is

---

Internet is the workplace of the 90s). Likewise, gambling is exploding in general and the Internet is its "newest frontier." *See* Scott M. Montpas, Comment, *Gambling On-line: For A Hundred Dollars, I Bet You Government Regulation Will Not Stop the Newest Form of Gambling*, 22 U. DAYTON L. REV. 163, 167-69 (1996).

[7] *See generally Nightline: Betting Without Borders [sic] The Odds of Stopping Gambling on the Internet* (ABC News television broadcast, Apr. 7, 1998), *available in* 1998 WL 5373021 (explaining that "policymakers are looking at a 21st century technology through 19th century eyes.").

[8] *See infra* Section II(A) (discussing the modern trend of holding an employer liable for the wrongful and illegal online activity of its employees).

[9] *See* John E. Davidson, *Reconciling The Tension Between Employer Liability and Employee Privacy*, 8 GEO. MASON U. CIV. RTS. L.J. 145, 180 (1998) (noting that the modern trend is to hold the employer liable without fault for its employee's wrongful or illegal activities); *see also* Joel M. Androphy et al., *General Corporate Criminal Liability*, 60 TEX. B.J. 121, 126-28 (1997) (recognizing that an employer may be held liable "even though the individual employee acted contrary to corporate policy or instructions.") (quoting *ACLU*, 929 F. Supp. at 831).

[10] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. at 459; *see also* Puathasnanon, *supra* note 4, at 694 (explaining the origins of the Internet, created by the United States Department of Defense).

[11] Puathasnanon, *supra* note 4, at 694 & n.29.

[12] *See* NUA Internet Surveys, *How Many Online* (last modified Mar. 28, 2000) <http://www.nua.ie/surveys/how_many_online/index.html> (explaining that, as of January 2000, there were approximately 248.6 million Internet users worldwide: 2.36 million in Africa; 42.6 million in Asia/Pacific; 64.23 million in Europe; 1.29 million in the Middle East; 131.1 million in Canada & USA; and 7.1 million in South America); *see also* NUA Internet Surveys, *Strategis Group: Over Half of US Adults Use the Internet* (visited Nov. 11, 1999) <http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905355395&rel=true> (explaining that half of the entire United States adult population are Internet users).

[13] *See Current Stats for Top Level Domains* ... (last modified Apr. 21, 2000)

that the Internet is accessible from anywhere (*e.g.*, at the office, home and while traveling).[14] In addition, electronic mail ("e-mail")[15] and Internet use in the workplace have experienced tremendous growth in the last five years.[16] Consequently, the workplace has become increasingly dependent on the Internet, and this dependence will continue through the new Millennium.[17]

6. The benefits produced by using the Internet and e-mail in the workplace are impressive. First, the Internet is a "revolutionary tool that dramatically affects the way we communicate, conduct business and access information."[18] The Internet provides access to a seemingly endless amount of information from various institutions, corporations, governments and individuals worldwide.[19] Furthermore, e-mail provides instant written communication between individuals, while eliminating the typical problems associated with mail, hand deliveries and the telephone.[20] In the workplace,

---

<http://www.netsizer.com/daily/TopLevelDomain.html>; *see also* NUA Internet Surveys, *ZD Marketing Intelligence: Internet Increase All Round* (visited Nov. 11, 1999) <http://www.nua.ie/surveys/index.cgi?f=VS&art_id=896362216&rel=true> (explaining that the "average [computer] is connected to the Internet about 4.5 hours per week.").

[14] *See* Puathasnanon, *supra* note 4, at 694.

[15] *See* ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996) (discussing use of e-mail). E-mail may be substituted for any purpose for which a person might use paper mail or a telephone for communication. *See* JOHN R. LEVINE ET AL., INTERNET FOR DUMMIES 11 (1993). It has now become the most popular and widely used service for users to exchange communications with each other, utilized by "millions of people all over the world." *Id*. Additionally, one person can reach many other users through mailing list services, newsgroups and numerous other Internet-related means of communication. *See ACLU*, 929 F. Supp. at 834. Also, e-mail messages can "carry attached files including word processing documents as well as graphical files of both still and action illustrations." David M. Clark, *… By Any Other Name …!*, STANDING COMM. ON LEGAL TECH., Illinois Bar Ass'n, Oct. 1998, at 3, 3.

[16] *See* Fernandez, *supra* note 6, at 833.

[17] *See id*. at 789.

[18] John T. Fojut, Legislative Update, *Ace In The Hole: Regulation of Internet Service Providers Saves the Internet Gambling Prohibition Act of 1997*, 8 DEPAUL-LCA J. ART & ENT. L. 155, 157 (1997) (quoting 143 Cong. Rec. E1633 (daily ed. Sept. 3, 1997) (statement of Rep. Bob Goodlatte).

[19] *See id*. at 158.

[20] *See* ACLU, 929 F. Supp. at 834; *see also* Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject A "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 412 (1997) (explaining the benefits of e-mail in the workplace, e.g., minimization of telephone tag, reducing "the problems posed by communication between different time zones," allowing "employees to find co-workers who have expertise on particular issues," and enabling "companies to put together teams of the best people without regard to location.").

"[e]-mail encourages intra company communication," while increasing employee productivity and reducing the need for inefficient forms of communication, e.g., "telephone calls, paper memos and face-to-face meetings."[21] Indeed, "[w]orkers use e-mail for more than just messages: E-mail can be used to send inventory lists, minutes of meetings, drafts of documents, business strategies, or records of important business decisions."[22] Thus, the employee can use the time saved to conduct other work-related tasks.[23]

7. Although the benefits of using technology in the workplace are experienced every day,[24] these benefits come with a price.[25] As employees increasingly gain access to the Internet and e-mail, the possibility for non-business and even illegal use increases as well.[26] For example, employees often send e-mail "messages that may be too candid to put in writing or" are merely inappropriate for the workplace.[27] E-mail systems are now capable of creating a complete and exact record of the communication,[28] and consequently, the employer's risk of liability has increased substantially from e-mail statements, such as an e-mail statement where a male

---

[21] Garry G. Mathiason & Michelle R. Barrett, *The Impact of New Technologies in the Workplace* (visited Oct. 10, 1999) <http://profs.findlaw.com/electronic/electronic_2.html>.

[22] *Id*.

[23] *See* Leib, *supra* note 20, at 412.

[24] *See id*.; *see also* Diana J.P. McKenzie, *Information Technology Policies: Practical Protection in Cyberspace*, 3 STAN. J.L. BUS. & FIN. 84, 100 (1997) (noting that the Internet and e-mail offer "significant advances in efficiency, productivity, and convenience").

[25] *See* Stuart Rosove, *Employee Internet Use and Employer Liability*, 1997 Employment Litig. Rep. (Andrews Pubs, Inc.) (Apr. 8, 1997), *available in* WESTLAW, ANEMPLR File (discussing a recently conducted CommerceNet Nielson spot telephone poll that revealed "that 66% of the people using the [Internet] had done so at work in the previous 24 hours . . . [and] the belief by many employers that their workers are using the Internet for entertainment on company time."); NUA Internet Surveys, *Pitney Bowes: Email is Changing the Working Day* (visited Nov. 11, 1999) <http://www.nua.ie/surveys/index.cgi?f=VS&art_id=897306427&rel=true> (explaining that the "[d]aily floods of e-mail are leaving 60 percent of executives, managers and professionals feeling overwhelmed . . . ."); NUA Internet Surveys, *BBC Online Network: Technology Proving A Work Distraction* (visited Nov. 11, 1999) <http://www.nua.ie/surveys/?f=VS&art_id=905354946&rel=true> (explaining "that the increasing amount of technology in use in the workplace is hindering productivity.").

[26] *See* Rosove, *supra* note 25.

[27] Mathiason & Barrett, *supra* note 21.

[28] *See id*. (explaining that "e-mail records usually store information regarding their transmission and receipt, including the names of the sender and recipient, the dates and time that the messages were sent and received, and an acknowledgment that the e-mail was retrieved.").

employee makes "frequent lewd remarks to a female employee via company e-mail."[29] Consequently, this technology has created expanding areas of potential liability for employers.[30]

B. Employer Liability

8. While the government does not want to restrict the advancement of technology in the workplace,[31] there is a strong public policy that imposes liability on employers for an employee's wrongful and illegal actions.[32] This policy stems from two deeply rooted concepts in the history of American corporations.[33] First, there is a general mistrust of corporate power.[34] Secondly, self-regulation is more efficient than government regulation.[35] Moreover, holding employers liable for their employees' wrongful and illegal actions provides another liable source, e.g., a deep pocket, from which a damaged party may recover damages; consequently, plaintiffs' attorneys are adding these potential claims against liable employers as defendants.[36]

---

[29] *Id.*

[30] *See* Rosove, *supra* note 25 (noting that "five areas of potential employer liability are beginning to emerge relating to employee Internet usage . . . : defamation; copyright infringement; sexual harassment; discrimination; and obscenity."); Mark Grossman, *Employee E-mail Presents Problems*, LEGAL TIMES, June 14, 1999, *available in* Law News Network (last modified June 22, 1999) <http://www.lawnewsnet.com/stories/A2282-1999Jun11.html>.

[31] *See* American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) (discussing the fact that "inconsistent legislation" could paralyze the advancement of technology).

[32] *See* Petro-Tech, Inc. v. Western Co. of N. Am., 824 F.2d 1349, 1358 (3d Cir. 1987) (explaining that the doctrine of respondeat superior "can probably be best explained as an outgrowth of the sentiment that 'it would be unjust to permit an employer to gain from the intelligent cooperation of others without being responsible for the mistakes, the errors of judgment and the frailties of those working under his direction and for his benefit.'") (quoting RESTATEMENT (SECOND) OF AGENCY § 219 (1958); *see also* Davidson, *supra* note 9, at 180 (noting that courts generally tend to impose "liability without fault" upon the employer).

[33] *See* Harvey L. Pitt & Karl A. Groskaufmanis, *Minimizing Corporate Civil and Criminal Liability: A Second Look at Corporate Codes of Conduct*, *in* ANNUAL TELECONFERENCE ON SECURITIES REGULATION 1990, at 319 (PLI Corp. Law and Prac. Handbook Series No. B4-6935, June 1990), *available in* WESTLAW, PLI/Corp File (discussing studies that have found that there are "two concepts deeply rooted in American economic history.").

[34] *See id.* (recognizing that, since the early years of America, there has been a general mistrust of corporations).

[35] *See id.* (recognizing that self-regulation "is preferable and more effective than government regulation . . . .").

[36] *See* Bradley J. Haight, *Civil RICO Section 1962(c): Vicarious Liability and Arguments for Expanding its Scope and Elements*, 15 Civ. Rico Litig. Rep. (Andrews Pubs., Inc.) 11 (May 1999),

9. Under the common law, an employer could be held liable for an employee's wrongful acts if the wrongful acts occurred "within the scope of the employee's employment."[37] The burden was placed on the employer to show that the employee's actions were not within the scope of his employment.[38] If the evidence presented left any questions of doubt, then it became an issue for determination by the fact finder.[39]

10. The Restatement of Agency reflects the court's traditional exposition of the scope of employment and provides that:

> (1) [the c]onduct of [an employee] is within the scope of employment if, but only if: (a) it is of the kind he is employed to perform; (b) it occurs substantially within the authorized time and space limits; (c) it is actuated, at least in part, by a purpose to serve the [employer], and (d) if force is intentionally used by the [employee] against another, the use of force is not [unforeseeable to the employer].[40]

11. Conversely, "[c]onduct of [an employee] is not within the scope of employment if it is different in kind from that authorized, far beyond the authorized time or space limits, or too little actuated by a purpose to serve [the employer]."[41]

12. However, the current trend of the courts expands the situations when an employer may be liable for the wrongful and illegal acts of its employees.[42] Two

---

available in WESTLAW, ANCRLR File.

[37] Martin v. Cavalier Hotel Corp., 48 F.3d 1343, 1348, 1352, 1360 (4th Cir. 1995) (affirming jury verdict ruling employer liable because employee was acting within the scope of employment); *see also* Fitzgerald v. Mountain States Tel. & Tel. Co., 68 F.3d 1257, 1263 (10th Cir. 1995) (discussing an employer's liability for punitive damages), *cited in* Daniels v. Worldcom Corp., No. Civ. A. 3:97-CV-0721-P., 1998 WL 91261, at *5 (N.D. Tex. Feb. 23, 1998); United States v. Gold, 743 F.2d 800, 822-23 (11th Cir. 1984); United States v. Cincotta, 689 F.2d 238, 241-42 (1st Cir. 1982), *quoted in* United States v. MacDonald & Watson Waste Oil Co., 933 F.2d 35, 42 (1st Cir. 1991); Standard Oil Co. of Texas v. United States, 307 F.2d 120, 127-28 (5th Cir. 1962); Commercial Bus. Sys., Inc. v. BellSouth Servs., Inc., 453 S.E.2d 261, 266 (Va. 1995) (reversing summary judgment ruling that employer was not liable because employee was not acting within the scope of employment); Smith v. Landmark Communications, Inc., 431 S.E.2d 306, 307-08 (Va. 1993) (noting that corporate liability under Virginia's respondeat superior doctrine is established when the "relationship of master and servant existed at the time and with respect to the specific action out of which the injury arose.").

[38] *See Commercial Bus. Sys., Inc.*, 453 S.E.2d at 265; *accord Martin*, 48 F.3d at 1351.

[39] *See* Orr v. William J. Burns Int'l Detective Agency, 12 A.2d 25, 27 (Pa. 1940); *see also* Bowman v. Home Life Ins. Co. of Am., 243 F.2d 331, 335 (3d Cir. 1957) (recognizing that the issue of whether a person acted within the scope of employment is ordinarily left to the jury).

[40] RESTATEMENT (SECOND) OF AGENCY § 228 (1958).

[41] *Id.*

[42] *See, e.g., Martin*, 48 F.3d at 1351; Domar Ocean Transp. v. Independent Refining Co., 783 F.2d

examples of cases demonstrating the modern trend of expanding the scope of employment, and specifically, the requirement that the employee be motivated, at least in part, by a purpose to serve the employer are *McNair v. Lend Lease Trucks, Inc.*,[43] and *Doe v. United States*.[44]

13. In McNair, the Fourth Circuit held that Lend Lease Trucks, Inc., could be held liable for a wrongful death caused by its employee.[45] The employee was a truck driver who, during working hours, went to a tavern and consumed enough drinks that his blood alcohol level was later found to be three times the legal limit.[46] A few hours later, the truck driver left the tavern, walked (or staggered) towards his truck, and stepped in front of the plaintiff's decedent who was driving a motorcycle.[47] Consequently, both the plaintiff and the truck driver died.[48] Lend Lease stipulated that the truck driver's three to four hour break could have been reasonable, and therefore, the truck driver was possibly acting within the scope of his employment.[49] However, whether the truck driver's break was reasonable, and if not, at what point he returned to the scope of his employment, were factual questions not appropriate for a motion to dismiss.[50]

14. Similarly, in *Doe*, the Eastern District of Virginia held an employer criminally liable for its employee's acts of sexual assault.[51] The court reasoned that

---

1185, 1190 (5th Cir. 1986); *Commercial Bus. Sys., Inc.*, 453 S.E.2d at 266; Androphy, et al., *supra* note 9, at 122; Davidson, *supra* note 9, at 176; *see also* Doe v. United States, 912 F. Supp. 193, 194-95 (E.D. Va. 1995); Gary T. Schwartz, *The Hidden and Fundamental Issue of Employer Vicarious Liability*, 69 S. CAL. L. REV. 1739, 1754, 1764-65 (1996) (recognizing employer's reluctance to assert the right to indemnify a claim against an employee).

[43] 95 F.3d 325, 328 (4th Cir. 1996).

[44] 912 F. Supp. at 195.

[45] 95 F.3d at 331.

[46] *See id.* at 327-28.

[47] *See id.*

[48] *See id.* at 328.

[49] *See id.* at 328-29.

[50] *See id.* at 331.

[51] 912 F. Supp. 193, 195 (E.D. Va. 1995). In *Doe*, a manager employed by a Veteran's Administration Hospital committed sexual assault during regular scheduled therapy sessions and during the hospital's recognized working hours. *See id.* at 194. The criminal act occurred in the psychologist's office, an office that the hospital provided for his "use to carry out the hospital's mission of psychiatric treatment." *Id.* Furthermore, the psychologist's acts were foreseeable because the hospital understood or should have understood the "potential for health care providers to sexually abuse their patients." *Id.* In fact, the majority of the public is cognizant of ethical codes prohibiting

because the criminal act was committed during office hours and at the workplace, a jury could find that the act was within the scope of the employment.[52] Another court noted that a sexual assault by a manager was foreseeable because the employer's policy prohibited such behavior.[53]

15. On this point, courts have expanded employer liability for foreseeable acts of its employees, even if the acts only benefited the employee.[54] One rationalization for

---

the mistreatment of vulnerable psychiatric patients. *See id.* at 194-95.

[52] *See id.* at 195.

[53] *See* Martin v. Cavalier Hotel Corp., 48 F.3d 1343, 1352 (4th Cir. 1995).

[54] *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 69, at 500-01 (5th ed. 1984) (noting that the liability is strict because the employer "has a more or less fictitious 'control' over the behavior of the servant . . . . "). In addition, when the plaintiff established the existence of an employer-employee relationship between the defendant and the actual tortfeasor-employee, "the burden is on the [employer] to prove that the [employee] was *not* acting within the scope of his employment when he committed the [tort] . . . ." Plummer v. Center Psychiatrists, Ltd., 476 S.E.2d 172, 174 (Va. 1996) (internal citations omitted). Moreover, if the evidence leaves the question in doubt it becomes an issue to be determined by the jury. *See, e.g.*, Doe v. United States, 912 F. Supp. 193, 195 (E.D. Va. 1995); Kemezy v. Peters, 622 N.E.2d 1296, 1298 (Ind. 1993); Stropes v. Heritage House Children's Ctr., 547 N.E.2d 244, 249 (Ind. 1989). *But see* Blakey v. Continental Airlines Inc., 730 A.2d 854, 856, 858, 868 (N.J. Super. Ct. App. Div. 1999) (holding that a female airline pilot who was the subject of several allegedly defamatory comments that were posted by her co-workers on the airline's bulletin board, the use of which was restricted to airline's flight crews, had no defamation claim against the airline based on the doctrine of respondeat superior because airline employees were not required to use the bulletin board).

Similarly, in trademark regulation, a franchisor may be liable for contributory trademark infringement even if the franchisor did not perform the infringing acts and further, the franchisor may be held liable for a single franchisee's infringement if it induces the infringement or even solely as a result of the franchisor's failure to exercise reasonable diligence to foresee or prevent the violation. *See, e.g.*, Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 853-54 (1982). *See generally* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, *passim* (1984) (regarding contributory infringement of copyrights); Belford v. Scribner, 144 U.S. 488, 507 (1892) (holding both a printer and publisher liable for copyright infringement); Chanel, Inc. v. Italian Activewear of Florida, Inc., 931 F.2d 1472, 1477 (11th Cir. 1991) (regarding corporate officer liability); Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845-47 (11th Cir. 1990) (regarding contributory infringement of copyrights); Casella v. Morris, 820 F.2d 362, 365 (11th Cir. 1987) (regarding contributory infringement of copyrights); Chi-Boy Music v. Towne Tavern, Inc., 779 F. Supp. 527, 530 (N.D. Ala. 1991) (regarding corporate officer liability for copyright infringement). *But see* Mini Maid Servs. Co. v. Maid Brigade Sys., Inc., 967 F.2d 1516, 1522 (11th Cir. 1992) (imposing liability only when a franchisor intentionally induces the franchisee's trademark infringement, or knowingly joined in the acts).

A similar rationale is the "willful blindness" doctrine. *See, e.g.*, United States v. Mapelli, 971 F.2d 284, 286 (9th Cir. 1992); United States v. Lara-Velasquez, 919 F.2d 946, 950-51 (5th Cir. 1990); United States v. de Luna, 815 F.2d 301, 302 (5th Cir. 1987); United States v. Jewell, 532 F.2d 697, 700-01 & n.7 (9th Cir. 1976). The doctrine may impose liability on a corporation for deliberately disregarding criminal activity. *See, e.g., Mapelli*, 971 F.2d at 286. If an employer deliberately remains ignorant to avoid knowledge of criminal conduct, then it will be subject to criminal liability. *See, e.g.*, United States v. St. Michael's Credit Union, 880 F.2d 579, 584 (1st Cir. 1989); United States

this view is that since "the employee's job created the opportunity for the employee to commit [the wrongful or illegal act],"[55] and gave the employee apparent authority,[56] the employer therefore possessed the requisite element of control.[57] In other words, the employer has "more or less fictitious 'control'" over the employee,[58] and therefore, any act of the employee is an act of the employer.[59]

16. In *Lyon v. Carey*, the Court of Appeals for the District of Columbia held Pep Line Trucking Company vicariously liable when its employee raped a customer of a furniture store for which Pep Line made deliveries.[60] Although the court reasoned that the evidence would not support a finding that Pep Line knew or should have known that its employee had any inclination to commit sexual assaults, the court held Pep Line vicariously liable because its employee's credentials as a deliveryman enabled him to enter the victim's residence.[61] The court reasoned that deliverymen "are likely to be in situations of friction with customers," and "these foreseeable altercations may precipitate violence" within the scope of employment with Pep Line Trucking.[62]

17. Recently, courts have affirmed the expanded employer liability for foreseeable acts of its employees, even if the acts only benefited the employee. For example, in *Davis v. Liberty Mutual Insurance Co.*, a Vermont federal district court held that the "injury arises in the course of employment when it occurs within a period of time when the employee is on duty and in a place where the employee may reasonably be expected to be while fulfilling the duties of his or her employment contract."[63] Similarly, in *Goff v. Teachers' Retirement System of State of Illinois*, an

---

v. Bank of New England, 821 F.2d 844, 855 (1st Cir. 1987).

[55] Davidson, *supra* note 9, at 179.

[56] *See* RESTATEMENT (SECOND) OF AGENCY § 8B (1958) (explaining that an employer may be held liable for its employee's unauthorized tortious action when the employer has given the impression that the employee has authority).

[57] *See* Richardson v. Hennly, 434 S.E.2d 772, 776 (Ga. Ct. App. 1993) (recognizing that an employer has the element of control over all acts arising in the workplace setting).

[58] KEETON ET AL., *supra* note 54, § 69, at 500; *see also* Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1148-49 (7th Cir. 1992) (holding that a flea market operator could be found liable for a vendor's trademark infringement if the operator exercised willful blindness).

[59] *See* RESTATEMENT (SECOND) OF AGENCY § 219(1) cmt. a ("[T]he act of the [employee] is the act of the [employer] . . . .") (internal quotations omitted).

[60] 533 F.2d 649, 652 (D.C. Cir. 1976).

[61] *See id.*

[62] *Id.* at 651.

[63] 19 F. Supp. 2d 193, 197 (D. Vt. 1998).

Illinois federal district court held that the injury can be said to "arise out of one's employment if its origin is in some way connected with the employment so that there is a causal connection between the employment and the . . . injury."[64]

18. Therefore, under the modern trend of respondeat superior, an employer may be held liable for an employee's wrongful act if: (1) the act occurred within the employee's scope of employment; and (2) the wrongful act was known or should have been known by the employer.[65]

III. ANALYSIS

19. The analysis portion of this Comment discusses the instances in which an employer may be liable for an employee's illegal online activity at the workplace. Second, this portion analyzes illegal employee computer activity and employer liability under a modern theory of respondeat superior. Finally, this Comment proposes several steps that all employers must take to avoid liability for its employee's illegal online activity.

A. Computer Crimes

1. Stock Manipulation -- and Its Secondary Effect, Cybersmearing

20. Over the last five years, the security market has seen tremendous growth due largely in part to the Internet. Recent reports estimate that over nine million people now have online investing accounts and by 2003, there will be $3.3 trillion in online brokerage assets.[66] This tremendous growth of online investors can be attributed to the ease of obtaining information available through the Internet. This information can now provide individuals with virtually complete on-demand knowledge concerning all aspects of investing that was previously only available to professional investors.

---

[64] 713 N.E.2d 578, 582 (Ill. App. Ct. 1999) (alteration in original) (internal quotations omitted).

[65] A competent plaintiff's attorney should never have a cause of action under the respondeat superior doctrine dismissed because it is a question of fact, which must be resolved by the jury. *See, e.g.*, Goldwater v. Metro-N. Commuter R.R., 101 F.3d 296, 300 (2d Cir. 1996). However, punitive damages against employers when their employees engage in wrongful conduct will only be awarded when the employer "recklessly employed or retained" an employee whose wrongful conduct was known to the employer prior to the commission of the wrongful conduct. RESTATEMENT (SECOND) OF TORTS, § 909, cmt. b (1979); *see also* White v. Ultramar, Inc., 88 Cal. Rptr. 2d 19, 24 (Cal. 1999) (holding that "the corporation was not responsible for punitive damages where it neither personally directed nor ratified the wrongful act.").

[66] *See generally* Commissioner Laura S. Unger, U.S. SEC, *Speech by SEC Commissioner: Technology Bytes the Securities Industry: The New Millennium Brings New Investors and New Markets* (last modified Mar. 15, 2000) <http://www.sec.gov/news/speeches/spch354.htm>.

21. Unfortunately, many of the characteristics that make the Internet an excellent means of obtaining information also provide new opportunities to manipulate the stock market. Creating "hype" and manipulating a certain security has become easier by posting false information on various Bulletin Board Systems ("BBS") (e.g., an Internet message board), newsgroups or through e-mail. Posting fraudulent information by using any of these tools is relatively inexpensive, capable of reaching millions of people and fairly easy to accomplish by a single person. Moreover, using the Internet for a market manipulation scheme is much more effective than traditional stock frauds because "the Internet's speed, low cost and relative anonymity give con artists access to an unprecedented number of innocent investors."[67] Consequently, stock manipulation via the Internet is increasing at a rapid rate.

22. In defining when the employer may be held liable for the employee's use of its technology to commit securities fraud, it is first necessary to examine the behavior that constitutes illegal manipulation of the securities market.

a. Employer Liability Based On Securities Law

23. If an employee of a company whose stock is publicly traded uses a BBS, an Internet chat room or e-mail to commit a stock manipulation scheme, there is at least a risk in some jurisdictions that the company could be sued under the theory of respondeat superior to answer for the employee's misconduct.[68] Under Rule 10b-5, promulgated under Section 10(b) of the Securities Act of 1934, to establish a primary claim of liablity for aiding and abetting, a plaintiff must prove:

> (1) that the defendant made an untrue statement of material fact, or failed to state a material fact; (2) that the conduct occurred in connection with a purchase or sale of security; (3) that the defendant made the statement or omission with scienter; and (4) that the plaintiff relied on the misrepresentation and sustained damages as a proximate result of the misrepresentation.[69]

---

[67] Chairman Arthur Levitt, U.S. SEC, *Speech by SEC Chairman: Plain Talk About On-Line Investing* (last modified May 4, 1999) <http://www.sec.gov/news/speeches/spch274.htm>.

[68] *See* Robert A. Prentice, *The Future of Corporate Disclosure: The Internet, Securities Fraud, and Rule 10b-5*, 47 EMORY L.J. 1, 77 (1998). "Even accurate disclosures could be viewed as illicitly 'selective' and," if acted upon by chat room participants, might "invite insider trading liability . . . ." *Id*.

[69] Anixter v. Home-Stake Prod. Co., 77 F.3d 1215, 1224-25 (10th Cir. 1996); *see also* Securities Exchange Act of 1934 § 10(b), 15 U.S.C.A. § 78j(b) (1997); 17 C.F.R. § 240.10b-5 (1999).

24. Since corporations and other entities can only act through their agents, courts must recognize liability under the respondeat superior doctrine and other principles of agency law as a source of primary liability.[70]

25. Applying the theory of respondeat superior, an employer may be liable for its employee's stock manipulation if: (1) the act occurred within the employee's scope of employment; and (2) the wrongful act was known or should have been known by the employer.[71]

26. However, there is a debate concerning whether employer liability is applicable in securities fraud cases. In *Central Bank of Denver v. First Interstate Bank of Denver*, the Supreme Court rejected aiding and abetting liability under the securities laws.[72] However, the *Central Bank of Denver* decision left open the possibility that a corporation could be held liable if any manipulation of the corporation's stock occurred as a primary violation of Rule 10b-5.[73] Legislation subsequently overruled the result in *Central Bank of Denver* and provided for aiding and abetting liability.[74] In *Seolas*

---

[70] *See* Seolas v. Bilzerian, 951 F. Supp. 978, 984 (D. Utah 1997); *see also* Gary D. Hoke, Jr., Litig. Rel. No. 16266, 70 SEC Docket 1187 (Aug. 30, 1999).

[71] *See generally supra* Section II(B) (discussing the modern theory of respondeat superior).

[72] 511 U.S. 164, 191 (1994); *accord* Chiarella v. United States, 445 U.S. 222, 235 (1980) (holding that trading securities without disclosing inside information does not violate Section 10(b) unless the trader has an independent duty to disclose); Santa Fe Indus., Inc. v. Green, 430 U.S. 462, 476 (1977) (holding that Section 10(b) does not prohibit "a breach of fiduciary duty by majority stockholders, without any deception, misrepresentation, or nondisclosure" because such an act is not manipulative or deceptive conduct); Ernst & Ernst v. Hochfelder, 425 U.S. 185, 197, 201 (1976) (recognizing that "manipulative or deceptive" language in Section 10(b) refers to "knowing or intentional misconduct" and refusing to expand scope of liability under Section 10(b) to include negligent misconduct); Converse, Inc. v. Norwood Venture Corp., No. 96 CIV. 3745(HB), 1997 WL 742534, at *3 (S.D.N.Y. Dec. 1, 1997). *But see* American Soc'y of Mechanical Eng'rs v. Hydrolevel Corp., 456 U.S. 556, 570-74 (1982) (finding that an agency theory of liability in the context of antitrust statutes was "most faithful to the congressional intent that the private right of action deter antitrust violations," and holding that a principal may be held liable for the antitrust violations of its agent).

[73] 511 U.S. at 191. In this regard, the majority of the jurisdictions have held that such a theory remains viable. *See, e.g.*, *In re* Centennial Techs. Litig., 52 F. Supp. 2d 178, 183 (D. Mass. 1999) (noting that "[t]he 'majority rule' circuits have at least implicitly read [the words 'any person' in § 10b of the Securities Act of 1934] as encompassing some kinds of vicarious liability."); *In re* Kidder Peabody Sec. Litig., 10 F. Supp. 2d 398, 407 (S.D.N.Y. 1998) (noting that primary liability would be appropriate where "defendants were the original and knowing source of a misrepresentation and that defendants knew or should have known that misrepresentation would be communicated to investors . . . .").

[74] *See, e.g.*, SEC v. Fehn, 97 F.3d 1276, 1282, 1283 (9th Cir. 1996) ("Section 104 of the Private Securities Litigation Reform Act thus authorizes SEC injunctive actions for the aiding and abetting of violations of Sections 10(b) and 15(d) and related regulations, and thereby reverses any impact *Central Bank* might have had on the SEC's power to enjoin aiding and abetting of these securities provisions."); *see also* United States v. Irwin, 149 F.3d 565, 570 (7th Cir. 1998) (explaining the three-part formula for aiding and abettor liability is "'knowledge of the illegal activity that is being aided

v. Bilzerian, a Utah federal district court held that respondeat superior is a legitimate basis for liability under Section 10(b) because the employer's status merits responsibility for the tortious actions of its employees.[75] The court reasoned that respondeat superior in such a case was consistent with the intent and purpose of the securities laws, "to promote full disclosure and discourage fraud in the securities markets."[76] In *Pollack v. Laidlaw Holdings, Inc.*, a New York federal district court denied the employer's motion to dismiss a Section 10(b) claim based on agency liability because such a theory was still available after *Central Bank*.[77] Thus, the legislative history of the Securities Exchange Act of 1934 and case law supports the theory of respondeat superior as a legitimate basis for liability arising from fraudulent stock

---

and abetted, a desire to help that activity succeed, and some act of helping.'") (citation omitted); Vento & Co. of New York, LLC v. Metromedia Fiber Network, Inc., No. 97 CIV.7751(JGK), 1999 WL 147732, at *12-13 (S.D.N.Y. Mar. 18, 1999); Infinity Investors Ltd. v. Subramaniam, No. Civ. A. 3:97-CV1703G, 1998 WL 47602, at *2 (N.D. Tex. 1998); Trustees of Boston Univ. v. ASM Communications, Inc., 33 F. Supp. 2d 66, 73 n.9 (D. Mass. 1998); State *ex rel*. Goettsch v. Diacide Distribs., Inc., 561 N.W.2d 369, 374 (Iowa 1997) (following Iowa Code section 502.503(1) that imposes secondary liability on any person who "materially aid[s] and abet[s] in the act or transaction constituting" the securities fraud defined in section 502.401).

There are also a number of pre-*Central Bank* decisions that had established respondeat superior as a viable theory of liability in Section 10(b) cases. *See, e.g.*, Hollinger v. Titan Capital Corp., 914 F.2d 1564, 1576 n.27 (9th Cir. 1990); Castleglen, Inc. v. Commonwealth Sav. Ass'n, 689 F. Supp. 1069, 1072 (D. Utah 1988); *accord In re* Atlantic Fin. Management, Inc. 784 F.2d 29, 32 (1st Cir. 1986) (holding that "[t]here are strong reasons for believing that the 'direct or indirect' language of the Securities Act encompasses . . . common law agency liability."); Kerbs v. Fall River Indus., Inc., 502 F.2d 731, 740-41 (10th Cir. 1974). These courts held that Section 20(a) of the 1934 Act, which provides for "controlling person" liability under Section 10(b), did not supplant common-law agency principles and was therefore not the exclusive source of secondary liability for Section 10(b) violations. *See* Securities Exchange Act of 1934 § 20(a), 15 U.S.C. § 78t(a) (1994). Section 20(a) provides:

> Every person who, directly or indirectly, controls any person liable under any provision of this chapter or of any rule or regulation thereunder shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable, unless the controlling person acted in good faith and did not directly or indirectly induce the act or acts constituting the violation or cause of action.

15 U.S.C. § 78t(a). Under this view, respondeat superior and other agency theories were valid bases of liability under Section 10(b) independent from Section 20(a). *See Hollinger*, 914 F.2d at 1576; *Castleglen*, 689 F. Supp. at 1072.

[75] 951 F. Supp. 978, 983 (D. Utah 1997); *see also* Peltz v. SHB Commodities, Inc., 115 F.3d 1082, 1088-89 (2d Cir. 1997) (noting in context of a commodities trading case that where there is actual authority, the principal is bound by the actions of its agent without an inquiry into the cases of apparent authority); AT&T v. Winback & Conserve Program, Inc., 42 F.3d 1421, 1429-32 (3d Cir. 1994).

[76] *Seolas*, 951 F. Supp. at 983.

[77] No. 90 Civ. 5788 (DLC), 1995 WL 261518, at *17 (S.D.N.Y. May 3, 1995).

manipulation.[78] Moreover, by explicitly including corporations in its definition of "person,"[79] Congress foresaw that corporations would be held liable under agency principles.[80] Therefore, as explained by the Third Circuit in *AT&T v. Winback & Conserve Program, Inc.*,:

> [C]ourts imposing liability on agency theories are not expanding the category of affirmative conduct proscribed by the relevant statute; rather, they are deciding on whose shoulders to place responsibility for conduct *indisputably proscribed* by the relevant statute. The principal is held liable not because it committed some wrongdoing outside the purview of the statute which assisted the wrongdoing prohibited by the statute, but because its status merits responsibility for the tortious actions of its agent.[81]

27. Therefore, respondeat superior liability is still applicable in securities fraud cases.[82] Moreover, the Supreme Court has acknowledged that the employer owns the communication equipment used at work and it is the employer's business that is being conducted on this equipment.[83] Because this equipment may also allow the employee

---

[78] *See generally In re* Atlantic Fin. Management, 784 F.2d 29, 32-33 (1st Cir. 1986); Paul F. Newton & Co. v. Texas Commerce Bank, 630 F.2d 1111, 1115-16 (5th Cir. 1980); Castleglen, Inc. v. Commonwealth Sav. Ass'n, 689 F. Supp. 1069, 1072 (D. Utah 1988); *see also* Prentice, *supra* note 68, at 77 n.345 (1998) (providing a list of cases addressing whether respondeat superior survived *Central Bank*).

[79] *See* Securities Exchange Act of 1934, 15 U.S.C. § 77b(2).

[80] *See AT&T*, 42 F.3d at 1431; *see also* Central Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164, 191 (1994) (recognizing that "[a]ny person or entity, including a lawyer, accountant, or bank, who employs a manipulative device or makes a material misstatement (or omission) on which a purchaser or seller of securities relies may be liable as a primary violator under 10b-5, assuming *all* of the requirements for primary liability under Rule 10b-5 are met.").

[81] 42 F.3d at 1430-32 (holding that *Central Bank*'s discussion of aiding and abetting should not be transplanted into the more settled realm of agency law in the conduct of a Lanham Act case).

[82] For further analysis, *see* Prentice, *supra* note 68, at 77 n.345; Anne C. Flannery & Kristine Zaleskas, *Damage Control: Managing The Inevitable Corporate Crisis*, *in* CORPORATE COMPLIANCE 1999, at 423, 425 (PLI Corp. L. & Prac. Handbook Series No. B0-008W, 1999), *available in* WESTLAW, PLI/Corp File.

There are also a number of other provisions of the Exchange Act of 1934 that arguably prohibit the manipulation of stock prices through false or misleading Internet communication, including: 1) Section 10(b), 15 U.S.C.A. § 78j(b) (1997); 2) Rule 10b-5, 17 C.F.R. § 240.10b-5 (1999); 3) Rule 10b-1, 17 C.F.R. § 240.10b-1 (1999); 4) Sections 9(a)(2)&(3), 15 U.S.C. A. § 78i(a)(2)-(3); and 5) Section 9(a)(4), 15 U.S.C.A. § 78i(a)(4).

[83] *See generally* O'Connor v. Ortega, 480 U.S. 709, 718-25 (1987) (upholding the search of a public employer's office and disruption to employee's personal belongings because "[g]overnment offices are provided to employees for the sole purpose of facilitating the work of an agency. The employee may

the opportunity to manipulate the corporate employer's stock value, the majority of the courts will hold the employer liable for its employee's act of stock manipulation because the act occurred within the scope of the employee's employment.[84]

28. Additionally, under the Racketeer Influenced and Corrupt Organizations Act ("RICO"),[85] an employer may also be penalized for its employee's manipulation of its stock value. Under RICO, racketeering activity includes activities by an enterprise that represents a pattern of racketeering activity or manipulation of a security, and that are indictable under other statutes such as those prohibiting securities fraud, wire fraud and fraud involving the use of mail.[86] RICO defines an "enterprise" as "any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity . . . ."[87] A "pattern of racketeering activity" is defined as "at least two acts of racketeering activity, one of which occurred after the effective date of this chapter and the last of which occurred within ten years . . . after the commission of a prior act of racketeering activity," and an "unlawful debt" is defined as "debt . . . incurred or contracted in gambling activity which was in violation of the law of the United States, a State or political subdivision thereof . . . and . . . which was incurred in connection with the business of gambling in violation of the law of the United States, a State or political subdivision thereof . . . ."[88] Thus, if an employee manipulates the company's stock value or gambles using the employer's technology while at the workplace, the employer may also be penalized under RICO.

b. Examples of Stock Manipulation Conduct By Employees

29. One possible stock manipulation scenario in the workplace can occur when employees, by using aliases or intermediaries, post rumors on the Internet to hype their company in connection with their personal purchase or sale of their company's stock.[89] In fact, "[r]umors posted on the Internet are especially damaging because they

---

avoid exposing personal belongings at work by simply leaving them at home.") (plurality opinion).

[84] *See generally* KEETON ET AL., *supra* note 54, § 69, at 499 (describing the theory of imputed negligence, which "means that, by reason of some relation existing between A and B, the negligence of A is to be charged against B, although B has played no part in it, . . . or indeed has done all that he possibly can to prevent it.").

[85] Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962 (1994).

[86] *See* David J. Beck, *Legal Malpractice in Texas*, 50 BAYLOR L. REV. 551, 802 (1998)

[87] 18 U.S.C. § 1961(4).

[88] *Id.* § 1961(5)-(6).

[89] *See* Blake A. Bell, *Reducing the Liability Risks of Employee Misuse of the Internet*, WALLSTREETLAWYER.COM, June 1999, at 16, 16.

are so easily spread."[90] Moreover, "[o]nce the rumor is posted in cyberspace, it takes on a life of its own."[91] For example, a "person who reads the rumor can forward it . . . [easily] to hundreds of friends [or] can post it on an Internet [BBS] where it will [be very likely to] be read by thousands of other people, each of whom can forward the rumor to all of his or her friends."[92] Furthermore, "[t]hese Internet rumors are impossible to control and can circulate on the Internet for years-long after the anger of the disgruntled employee who posted the rumor has subsided."[93]

30. For example, in April of 1999, Gary D. Hoke, a 25-year old PairGain Technologies employee, posted a false message on a Yahoo! Finance message board that said "'BUYOUT NEWS!!! ECILF is buying [PAIRGAIN TECHNOLOGIES] . . . . Just found it on Bloomberg.'"[94] The posting also included a "hyperlink to a Web page that appeared to be part of Bloomberg L.P.'s news site."[95] The linked-to page contained "an 'announcement' that PairGain was being acquired by ECI Telecom Ltd., an Israeli company, in a transaction with 'an implied value of $1.35 billion,' including the 'equity purchase price as well as a technology development incentive plan.'"[96] As a result, PairGain's stock price quickly rose from $8 1/2 to $11 1/8, an approximate thirty-one percent increase, before the markets returned to normal and the price of PairGain's shares dropped back.[97] After the public realized that Hoke's message was false, Bloomberg L.P., the Los Angeles U.S. Attorney's Office, and the Securities and Exchange Commission ("SEC") each filed separate lawsuits against Hoke.[98] As a result of his stock manipulation scheme, Hoke faced claims of securities fraud for manipulating the price of PairGain's publicly traded securities in violation of the Securities Exchange Act of 1934 and Rule 10b-5.[99] Hoke pleaded guilty to posting the

---

[90] Garry G. Mathiason, *CyberSabotage--The Internet as a Weapon in the Workplace: Internet Zone One (Cont'd)* (visited Feb. 18, 2000) <http://profs.findlaw.com/networked/networked_6.html> (describing detrimental effects companies suffer as a result of third party reliance on Internet bulletin boards).

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *See* Bell, *supra* note 89.

[95] *Id.*

[96] *Id.*

[97] *See id.* at 16-17.

[98] *See* Gary D. Hoke, Jr., Litig. Rel. No. 16266, 70 SEC Docket 1187 (Aug. 30, 1999).

[99] *See id.*

fake corporate takeover story on the Internet and as a result was initially required to pay more than $93,000 to his victims, and placed on probation for five years.[100]

31. Through all of this, PairGain cooperated in the investigation, during which there were no allegations that anyone other than Hoke was involved in the scheme.[101] Nonetheless, "there can be little doubt that the company suffered through anxious moments, worried about liabilities that it might face as a result of the misguided scheme implemented by a 25-year old 'mid-level' engineer employed in its North Carolina development facility."[102]

32. Another likely scenario can occur when employees of e-brokerage firms actively participate in investor chat rooms. For example, "[I]f an employee of an e-broker actually uses a chat room to commit securities fraud, through a stock manipulation scheme or otherwise, there is at least a risk . . . that the e-broker could be sued, under a theory of respondeat superior" due to its employees' misconduct.[103]

33. Yet another likely scenario occurs when employees register their viewpoints about their corporate employer on a chatroom that intentionally or unintentionally manipulates investors to buy or sell their shares in the corporation's stock.[104] The power of a false rumor to manipulate images was demonstrated in *Zeran v. America Online, Inc.*[105] Although this case did not involve a disgruntled employee, a situation like the one described in this case could easily occur between an employee and employer.[106] An anonymous individual posted a false advertisement on an American Online bulletin board, listing Mr. Zeran's name and phone number.[107] The ad was offensive, caused angry phone calls and death threats, and attracted the attention of a local radio station.[108] America Online would not remove the ad, and Zeran

---

[100] *See id.* (noting that the proposed final judgement did not include a monetary penalty); Associated Press, *Man Gets Probation and Home Detention in Online Stock Hoax* (visited Apr. 10, 2000) <http://search.nytimes.com/search/daily/homepage/bin/fastweb?getdoc+cyber-lib+cyber-lib+6036+0+wAAA+hoke>; John Swartz, *Man Gets Probation in Web Fraud Case*, WASHINGTON POST, Aug 31, 1999, at E3.

[101] *See* Bell, *supra* note 89, at 17.

[102] *Id.*

[103] Blake A. Bell, *E-Broker Chat Rooms and Federal Securities Laws*, WALLSTREETLAWYER.COM, Aug. 1998, at 1.

[104] *See id.* (discussing potential liability of e-brokers for the actions of third-party content providers).

[105] 129 F.3d 327 (4th Cir. 1997).

[106] *See id.* at 329.

[107] *See id.*

[108] *See id.*

subsequently sued.[109] However, Zeran lost his case because the theory for his recovery, the Communications Decency Act,[110] barred his cause of action.[111] It is obvious that posting false statements on the Internet can not only manipulate a corporate employer's stock value, but also "cybersmear" the employer.[112]

c. The Secondary Effect of Stock Manipulation, Cybersmearing

34. "Cybersmearing" is the posting of a false and damaging statement over the Internet.[113] Employers need to be aware of the risk of this kind of cybersabotage because they need to react quickly in order to minimize the damage if it should happen to them.[114]

35. Although the stories spread through cybersmearing are false, they cause real damage to the targeted employers.[115] Several Websites list and disprove false Internet rumors.[116] "However, by the time such rumors are dispelled, irreparable damage to a company's reputation often has already been done."[117] One commentator has described examples of such harm:

> Blue Mountain Arts, a small, family-owned business that offers free electronic greetings cards was recently devastated by a false Internet rumor. Someone posted a rumor on the Internet that Blue Mountain greeting cards contained a virus that would destroy the recipient's computer system when the card was opened. Tommy Hilfiger, a clothing designer, was also the victim of a false Internet rumor. The rumor stated that the designer said on the Oprah Winfrey

---

[109] *See id.*

[110] Communications Decency Act, 47 U.S.C. § 230 (1994 & Supp. 1998) (barring lawsuits that seek to treat interactive computer services providers "as the publisher or speaker of any information provided by another information content provider."). This Act effectively prevents "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions -- such as deciding whether to publish, withdraw, postpone or alter content . . . ." *Zeran*, 129 F.3d at 330.

[111] *See Zeran*, 129 F.3d at 334-35.

[112] *See* Mathiason, *supra* note 90.

[113] *See id.*

[114] *See id.*

[115] *See id.*

[116] *See id.* One such site is *Urban Legends and Folklore* (visited Mar. 23, 2000) <http://urbanlegends.miningco.com/culture/urbanlegends/>. *See id.*

[117] *Id.*

> Show that he wished minorities would not buy his clothing. The Internet message asked everyone who read it to boycott Tommy Hilfiger clothing. False Internet rumors about Taco Bell being infested with roaches and about Kentucky Fried Chicken deep-frying rodents have been circulating on the Internet for years. While it is not known if disgruntled employees were behind any of these rumors, they likely could have been. The Internet is a powerful tool and when used by an angry employee, it can destroy a company's reputation.[118]

2. Copyright Infringement

36. Enormous amounts of the material that can be found on the Internet are subject matter protected by the copyright laws of the United States.[119] Moreover, today's technology allows Internet users not only the opportunity to access, upload and download simple text, "but also allows [these] users [the opportunity] to do the same with pictures, movies, software, musical works, multimedia works and audiovisual works."[120] However, any copying of these works in violation of the exclusive rights provided by copyright law would clearly constitute copyright infringement under federal law.[121] Yet, copyright infringement activity on the Internet is also increasing at a rapid rate.[122]

37. In defining when the employer may be held liable for the employee's use of its technology to infringe the rights of a copyright owner, it is necessary to first examine the behavior that constitutes copyright infringement.

a. Employer Liability Based On Copyright Law

38. Under copyright law, an employer may be held liable for copyright infringement committed by one of its employees, even when an employer did not actually perform the copying or distributing.[123] First, under the theory of respondeat superior, an employer may be liable for its employee's infringement if: (1) the act

---

[118] *Id*.

[119] *See* Copyright Act, 17 U.S.C. § 102 (1994) (defining copyrightable subject matter).

[120] David N. Weiskopf, *The Risks Of Copyright Infringement On The Internet: A Practitioner's Guide*, 33 U.S.F. L. REV. 1, 3 (1998).

[121] *See id*. (citing Copyright Act, 17 U.S.C. § 106(1)-(5)).

[122] *See generally* United States Department of Justice, *Justice Department, F.B.I. and Customs Service to Combat Intellectual Property Crime* (last modified Apr. 12, 2000) <http://www.usdoj.gov/opa/pr/1999/July/323civ.htm> (explaining that United States Law Enforcement will target high tech corridors to fight the surge in intellectual property "piracy and online distribution of counterfeit products . . . .").

[123] *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

occurred within the employee's scope of employment; and (2) the wrongful act was known or should have been known by the employer.[124] Second, under the theory of vicarious liability, an employer may be liable for infringement committed by its employee if the employer: (1) had the right to supervise the employee's infringing activities; and (2) had a direct financial interest in such infringing activities, even when the employer had no knowledge of the infringement nor intent to infringe.[125] Third, under the theory of contributory infringement, an employer may be liable for infringement committed by its employee if: (1) the employer had knowledge of the infringing activity; and (2) the employer induced or materially contributed to the infringing conduct.[126]

---

[124] *See, e.g.*, Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1163 (2d Cir. 1971) (impliedly recognizing the respondeat superior rule for copyright infringement by applying vicarious liability as subset of respondeat superior); Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963) (recognizing that the respondeat superior rule applies to copyright infringement); Wihtol v. Crow, 309 F.2d 777, 782-83 (8th Cir. 1962) (finding defendant acting in scope of employment and employer jointly liable under respondeat superior); Bradbury v. Columbia Broad. Sys., Inc., 287 F.2d 478, 485 (9th Cir. 1961) (recognizing the rule by implication); Bourne v. Fouche 238 F. Supp. 745, 747 (E.D.S.C. 1965) (applying common law doctrine); Shapiro, Bernstein & Co. v. Veltin, 47 F. Supp. 648, 649 (W.D. La. 1942) (recognizing the rule by implication in case holding restaurant owner liable for copyright infringement even though music was played on his premises contrary to his objections); Buck v. Cecere, 45 F. Supp. 441, 441 (W.D.N.Y. 1942) (same); Buck v. Coe, 32 F. Supp. 829, 830 (M.D. Pa. 1940) (recognizing the rule by implication); M. Witmark & Sons v. Calloway, 22 F.2d 412, 414 (E.D. Tenn. 1927) (applying common law rule); M. Witmark & Sons v. Pastime Amusement Co., 298 F. 470, 475 (E.D.S.C. 1924), *aff'd* 2 F.2d 1020 (1924) (recognizing the rule by implication).

Courts have even held the employer liable under the respondeat superior doctrine for a copyright infringement committed by an employee after the employee acts against the employer's orders. *See, e.g.*, *Calloway*, 22 F.2d at 414 (recognizing the rule); *Bourne*, 238 F. Supp. at 747; *Veltin*, 47 F. Supp. at 649; *Cecere*, 45 F. Supp. at 441 (recognizing the rule by implication); *Coe*, 32 F. Supp. at 830 (recognizing the rule by implication).

[125] *See, e.g.*, *H.L. Green Co.*, 316 F.2d at 307; Microsoft Corp. v. Grey Computer, 910 F. Supp. 1077, 1090-91 (D. Md. 1995); Realsongs v. Gulf Broad. Corp., 824 F. Supp. 89, 91 (M.D. La. 1993); Universal City Studios, Inc. v. Nintendo Co., 615 F. Supp. 838, 857 (S.D.N.Y. 1985); L & L White Metal Casting Corp. v. Cornell Metal Specialties Corp., 353 F. Supp. 1170, 1175 (E.D.N.Y. 1972); Roy Export Co. Establishment v. Trustees of Columbia Univ., 344 F. Supp. 1350, 1352 (S.D.N.Y. 1972) (applying the vicarious liability rule to copyright infringement).

[126] *See, e.g.*, Sony Corp. of Am. v. Universal City Studios Inc., 464 U.S. 417, 487 (1984); Matthew Bender & Co., Inc. v. West Publ'g Co., 158 F.3d 693, 706 (2d Cir. 1998), *cert. denied*, 119 S.Ct. 2039 (1999) (explaining that there are two types of contributory infringement: "personal conduct that encourages or assists the infringement; and [providing the use of] machinery or goods that facilitate the infringement."); Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845 (11th Cir. 1990); *Gershwin Publ'g Corp.*, 443 F.2d at 1162; Burdick v. Koerner, 988 F. Supp. 1206, 1209 (E.D. Wis. 1998); Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 514 (N.D. Ohio 1997); Compaq Computer Corp. v. Procom Tech., Inc., 908 F. Supp. 1409, 1424 (S.D. Tex. 1995); Metzke v. May Dep't Stores Co., 878 F. Supp. 756, 760 (W.D. Pa. 1995); Sega Enters., Ltd. v. Maphia, 857 F. Supp. 679, 686 (N.D. Cal. 1994); Broadcast Music, Inc. v. Jeep Sales & Serv. Co., 747 F. Supp. 1190, 1194 n.1 (E.D. Va. 1990); Telerate Sys., Inc. v. Caro, 689 F. Supp. 221, 228 (S.D.N.Y. 1988)

39. For example, in *Playboy Enterprises, Inc. v. Webbworld, Inc.*, a Texas federal district court held Webbworld, an Internet service provider which sold adult images that were obtained from various newsgroups, vicariously liable for its employees' infringements of Playboy's copyrights.[127] The court reasoned that Webbworld: (1) had full control of day-to-day operations of its Website; (2) created and controlled the operation software that was the heart of the enterprise; and (3) selected the newsgroups it would use as sources of material, in return for which one of the principal defendants collected fifty percent of the net profits.[128]

40. In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, a California federal district court held that sufficient evidence existed such that a jury could reasonably find Netcom contributorily liable for a third party's infringing posting that passed through Netcom's network.[129] In this case, Netcom, an Internet service provider, was initially unaware of the infringing activity, but later received notice of the infringing activity from Religious Technology.[130] The court reasoned that this notice was sufficient to raise the issue of Netcom's responsibility to verify Religious Technology's allegation of infringing activity occurring on its system.[131]

41. Therefore, if an employer is in possession of improperly obtained software or other copyrighted material, it may be accused of copyright infringement under theories including the respondeat superior doctrine, vicarious liability or contributory liability.

(providing that for contributory infringement in copyright, the plaintiff must show "defendant's product has no 'substantial noninfringing uses.'") (citation omitted); Nick-O-Val Music Co., Inc. v. P.O.S. Radio, Inc., 656 F. Supp. 826, 828 (M.D. Fla. 1987); Southern Mississippi Planning & Dev. Dist., Inc. v. Robertson, 660 F. Supp. 1057, 1062 (S.D. Miss. 1986); Schuchart & Assocs. v. Solo Serve Corp., 220 U.S.P.Q. (BNA) 170, 176 (W.D. Tex. 1983); Amusement Co., Inc., 551 F. Supp. 104, 108 (N.D. Ill. 1982) (discussing personal liability of business owners); Aitken, Hazen, Hoffman, Miller, P.C. v. Empire Constr. Co., 542 F. Supp. 252, 257 (D. Neb. 1982); Broadcast Music, Inc. v. Fox Johnson v. Salomon, 197 U.S.P.Q. (BNA) 801, 829 (D. Minn. 1977); Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F. Supp. 399, 403 (S.D.N.Y. 1966).

127 991 F. Supp. 543, 554 (N.D. Tex. 1997).

128 *See id.*

129 907 F. Supp. 1361, 1371, 1382 (N.D. Cal. 1995) (presenting facts sufficient to raise a question as to Netcom's knowledge once it received a letter from Religious Technology informing it of the allegedly infringing activity on its network).

130 *See id.* at. 1374.

131 *See id.* at 1374-75, 1382.

b. Examples of Copyright Infringement Conduct By Employees

42. If an employer has "[a] copy of a software program that cannot be validated by purchasing records[,] . . . an allegation of copyright infringement" may be brought against it.[132] "This can be caused by software that was brought in from an employee's home, or was created by conscientious employees trying to get a job done more efficiently [via the Internet]. Or, perhaps the software was an unauthorized copy created by a well-meaning but misguided cost-conscious manager."[133]

43. For example, in *Marobie-FL, Inc. v. National Association of Fire Equipment Distributors*, an Illinois federal district court held a trade organization liable for copyright infringement after one of its employees who was responsible for its Website adorned the site with copyrighted clip art.[134] The court reasoned that the trade organization could not rely on an "innocent infringer" defense, because such a defense may only be raised "when the infringer relied on an authorized copy that omitted the copyright notice," and "[i]n this case [the defendant's employee] relied on unauthorized copies of plaintiff's clip art files."[135] Thus, "the risks of online copyright claims as a result of employee misconduct [are] very real."[136] "The nature of the Internet makes it easy to copy and to forward or publish copyrighted images or content."[137] Further, "as the National Association of Fire Equipment Distributors discovered, liability can result from what may otherwise seem to be the most innocent of activities."[138]

44. Another issue that employers must be concerned about is the fact that:

> [c]opyright infringement settlements can be expensive. For example, suppose there is an average of two illegal programs per computer, with an average cost of one hundred dollars, and assume that there are five hundred machines within an organization's headquarters and branch offices. The cost of purchasing legitimate copies of the illegal software

---

[132] Mathiason & Barrett, *Employment Law Implications and Solutions (Cont'd)* (visited Feb. 2, 2000) <http://profs.findlaw.com/electronic/electronic_18.html>.

[133] *Id.*

[134] 983 F. Supp. 1167, 1171, 1176 (N.D. Ill. 1997).

[135] *Id.* at 1174.

[136] Bell, *supra* note 89, at 18; *see also* Broadcast Music, Inc. v. The Club S. Burlesque Inc., 36 U.S.P.Q.2d (BNA) 1664, 1666 (N.D. Ga. 1995) (holding a nightclub owner vicariously liable for infringement of copyrighted musical composition by dancers, who were independent contractors, that played recordings of infringed songs in the nightclub).

[137] Bell, *supra* note 89.

[138] *Id.*

> might be one hundred thousand dollars. [Moreover, p]enalties are usually one to two times the retail value of the illegal software.[139]

c. Employer Liability Based On Trademark and Trade Secret Laws

45. These rationales for holding an employer liable for its employee's copyright infringement, e.g., respondeat superior doctrine, vicarious liability and contributory liability, can also be applied to both trademark[140] and trade secret[141] laws. For example, if employees post a third party's trademark on their employer's web site, and the employer failed to take remedial action once it received notification of the trademark violation, the employer may be held liable for its employee's trademark infringement either under the respondeat superior doctrine, vicarious liability or contributory liability.[142] Likewise, if employees use their employer's technology, e.g., a computer, computer disk, Internet access, telephone or e-mail, to obtain proprietary information from a third party, e.g., a customer list, software program or secret formula, the employer may be held liable for its employee's misappropriation of a third party's trade secrets either under trademark or trade secret law.[143] The contributory liability doctrine will apply if the employer had notice of the trade secret violation "and induced or materially contributed to the infringing conduct."[144] The vicarious liability theory will apply "if the employer had the right and the ability to supervise the employee's activity, and had a financial interest in exploitation of the [trademarked or trade secret] materials."[145]

---

139 Mathiason & Barrett, *supra* note 132.

140 *See generally* Lanham Act, 15 U.S.C. § 1051 *et seq*. (1994 & Supp. 1999).

141 *See generally* Economic Espionage Act of 1996, 18 U.S.C. § 1831 *et seq*. (1994 & Supp. IV 1999) (providing examples of third party liability for trade secret misappropriation); R. Mark Halligan, *Third-Party Liability for Trade Secret Misappropriation* (last modified Apr. 3, 1998) <http://www.execpc.com/~mhallign/3party.html> (identifying key definitions regarding the theft of trade secrets under the Uniform Trade Secrets Act, § 1, 14 U.L.A. 437 (1990)).

142 *See generally* Deborah F. Buckman, Annotation, *Liability as Vicarious or Contributory Infringer Under the Lanham Act – Modern Cases*, 152 A.L.R. FED. 573 (1999) (explaining that the common law theories of contributory liability and vicarious liability apply to trademark infringement).

143 *See* Halligan, *supra* note 141 (noting that a group of investors forming a company could be liable for trade secret misappropriation by employees joining the new company who disclose trade secrets from their previous company to the investors). *See generally* Thomas P. Klein, *Electronic Communications in the Workplace: Legal Issues and Policies*, *in* THIRD ANNUAL INTERNET LAW INSTITUTE, at 695, 719-20 (PLI Pat., Copyrights, Trademarks, & Literary Prop. Course Handbook Series No. G0-0051, 1999), *available in* WESTLAW, PLI/Pat File (describing an employer's potential liability for an employee's copyright infringement).

144 Mathiason & Barrett, *supra* note 132.

145 *Id*.

3. Computer Viruses and Worms

46. When computer viruses and worms are executed, they destroy data found in their hosting computer system.[146] Moreover, after infecting a computer system, both computer viruses and worms may then use the Internet to find additional hosts to spread their infection.[147] If employees, while at their workplace, introduce computer viruses and worms into electronic commerce, their employers may be held liable for the damage caused by this introduction.[148] However, a fundamental understanding of computer viruses and worms is required in order to understand this type of potential employer liability.

47. First, a computer virus is a portion of a computer code that affixes itself to other computer codes located in a computer system, e.g, software application codes that are used to boot a computer or macro instructions embedded in documents.[149] The computer virus is thereby activated by any action that causes the infected computer code to run, e.g., "turning on a computer, starting an application, or opening an e-mail attachment . . . ."[150] This activation occurs because the computer virus is affixed in such a manner to its hosting computer code that it causes the virus to be activated first "when the host is loaded . . . for execution . . . ."[151] Thereafter, the computer virus multiplies itself by looking for additional uninfected hosts and affixing a copy of itself to them.[152]

48. Second, a computer worm is a program that spreads itself "from one computer to another [through the use of] a computer network."[153] Unlike computer viruses, computer worms do not get any assistance from unsuspecting users.[154] They must locate a computer system that "they can penetrate, carry out an attack, and transfer a replica of their code to the target host for execution."[155] Thus, a computer

---

146 *See* DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 269 (1999).

147 *See id.* at 269, 273, 280.

148 *See infra* Section 3(a).

149 *See* DENNING, *supra* note 146, at 269-70.

150 *Id.*

151 *Id.* at 269-70.

152 *See id.*

153 *Id.* at 280.

154 *See id.*

155 *Id.*

worm is simply a program that computerizes all of the necessary steps needed to break from one computer system into the next.[156]

49. The next step needed to define when an employer may be held liable for its employee's use of the a computer at the workplace to release a computer virus or worm onto the Internet is to identify a specific legal theory which provides respondeat superior liability in such a situation.

a. Employer Liability Based On The Computer Fraud and Abuse Act

50. The advent of computer viruses and worms are perhaps the scenarios Congress envisioned when it enacted the precedent Computer Fraud and Abuse Act of 1986 ("CFAA").[157] Under the CFAA, "[w]hoever . . . 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" may face five to ten years in prison and/or monetary fines under the CFAA.[158] Furthermore, under the CFAA, persons who suffer harm as the result of illegal access or damage to a protected computer have a private right of action against the person who caused the harm.[159]

51. In terms of prosecuting the originators of computer viruses and worms,[160] there exists interesting precedental case law under the CFAA. For example, in *U.S. v. Kashpureff*, the self-proclaimed "webslinger" defendant designed a computer virus that infected a computer system that allowed "Internet-linked computers to communicate with each other."[161] Once the computer virus was launched, Internet

---

156 *See id.*

157 Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 *et seq.* (1994 & Supp. IV 1999). The 1986 Act amended the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. *See id.*; Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190.

158 18 U.S.C. § 1030(a)(5)(A), (c)(3)(A)-(B).

159 *See id.* § 1030(g). "Protected computers" are defined as computers being "used in interstate commerce or communication" or by "a financial institution or the United States Government . . . ." *Id.* § 1030(e)(2). *See generally* Mark Ishman & Quincy Maquet, *A Consumer's Analysis of the Electronic Currency System and the Legal Ramifications for a Transaction Gone Awry*, 6 MURDOCH UNIV. ELECTRONIC J.L. 3, ¶¶ 79-83 (Sept. 1999) <http://www.murdoch.edu.au/elaw/issues/v6n3/ishman63_text.html> (discussing the prosecution of the author of a computer worm which crashed 6,000 computers).

160 *See generally* Matt Lake, *Cracking the Charts: The Ten Most Subversive Hacks of All Time,* CNET (visited Apr. 21, 2000) <http://www.cnet.com/specialreports/0-6014-7-1420567.html?tag=st.cn.sr1.dir.>.

161 Patricia Hurtado, *Internet Hijacking / 'Webslinger' Enters Guilty Plea*, NEWSDAY, Mar. 20, 1998, at A40, *available in* 1998 WL 2663136; *see also* Lake, *supra* note 160.

users that attempted to reach the defendant's major competitor, Internic, were instead linked to the defendant's commercial Internet site.[162] As a result, the defendant pleaded guilty to the CFAA charges, and now faces a maximum sentence of five years in prison and a maximum fine of $250,000.[163]

52. In addition to the sanctions under the CFAA, the originator of the computer virus and worms might face potential prosecution under other federal statutes, such as the U.S. wire fraud laws.[164] Additionally, a substantial number of states have enacted legislation that addresses computer-related crime.[165]

b. Examples of Viruses And The Potential Liability To Employers

53. One of the latest Internet viruses was unleashed on March 26, 1999, when the "Melissa Macro Virus" was posted to the "alt.sex." newsgroup.[166] In just a few days,

---

[162] *See* Hurtado, *supra* note 161.

[163] *See id.*

[164] *See* Wire Fraud Act, 18 U.S.C. § 1341 *et seq.*; *see also* Mail Fraud Act, 18 U.S.C. § 1343 *et seq.*

[165] *See, e.g.*, ALA. CODE §§ 13A-8-100 to -103 (1994); ALASKA STAT. § 11.46.200(3) (Michie 1998); ARIZ. REV. STAT. ANN. § 13-2316 (West 1989 & Supp. 1999); ARK. CODE ANN. §§ 5-41-101 to -107 (Michie 1997); CAL. PENAL CODE § 502 (West 1999 & Supp. 2000); COLO. REV. STAT. §§ 18-5.5-101 to -102 (1999); CONN. GEN. STAT. ANN. §§ 53a-250 to -261 (West 1994 & Supp. 1999); DEL. CODE ANN. tit. 11, §§ 931-939 (1995 & Supp. 1998); FLA. STAT. ANN. §§ 815.01-.07 (West 1993 & Supp. 2000); GA. CODE ANN. §§ 16-9-90 to -94 (1999); HAW. REV. STAT. ANN. §§ 708-890 to -893 (Michie 1999); IDAHO CODE §§ 18-2201 to -2202 (1997); 720 ILL. COMP. STAT. 5/16D-1 to -6 (formerly ILL. REV. STAT. 1991, ch. 38, ¶ 16D-1 to -6) (West 1993); IND. CODE ANN. §§ 35-43-1-4, 35-43-2-3 (West 1998); IOWA CODE ANN. §§ 716A.1-.16 (West 1993); KAN. STAT. ANN. § 21-3755 (1995 & Supp. 1999); KY. REV. STAT. ANN. §§ 434.840 to .860 (Michie 2000); LA. REV. STAT. ANN. §§ 14:73.1-.5 (West 1997 & Supp. 2000); ME. REV. STAT. ANN. tit. 17-A, §§ 431-433 (West 1983 & Supp. 1999); MD. ANN. CODE art. 27, § 146 (Supp. 1999); MASS. GEN. LAWS ANN. ch. 266, § 30 (West 1990 & Supp. 1999); MICH. COMP. LAWS ANN. §§ 752.791-.797 (West 1991 & Supp. 1999); MINN. STAT. ANN. §§ 609.87 to .893 (West Supp. 2000); MISS. CODE ANN. §§ 97-45-1 to -13 (1999); MO. ANN. STAT. §§ 569.093-.099 (West 1999); MONT. CODE ANN. §§ 45-6-310 to -311 (1999); NEB. REV. STAT. §§ 28-1343 to -1348 (1995); NEV. REV. STAT. §§ 205.473-491 (1999); N.H. REV. STAT. ANN. §§ 638:16 to :19 (1996); N.J. STAT. ANN. §§ 2C:20-23 to -34 (West 1995); N.M. STAT. ANN. §§ 30-45-1 to -7 (Michie 1997); N.Y. PENAL LAW §§ 156.00-.50 (McKinney 1988 & Supp. 1998); N.C. GEN. STAT. §§ 14-453 to -457 (1999); N.D. CENT. CODE § 12.1-06.1-08 (1999); OHIO REV. CODE ANN. § 2913.04 (Anderson 1993); OKLA. STAT. ANN. tit. 21, §§ 1951-58 (West Supp. 2000); OR. REV. STAT. §§ 164.125, 164.377 (1997); 18 PA. CONS. STAT. ANN. § 3933 (West Supp. 1999); R.I. GEN. LAWS §§ 11-52-1 to -8 (1994 & Supp. 1999); S.C. CODE ANN. §§ 16-16-10 to -40 (Law. Co-op. 1985 & Supp. 1999); S.D. CODIFIED LAWS §§ 43-43B-1 to -8 (Michie 1997); TENN. CODE ANN. §§ 39-14-601 to -603 (1997); TEX. PENAL CODE ANN. §§ 33.01-.05 (West 1994 & Supp. 2000); UTAH CODE ANN. §§ 76-6-701 to -705 (1999); VA. CODE ANN. §§ 18.2-152.2 to .4 (Michie 1996 & Supp. 1999); WASH. REV. CODE ANN. §§ 9A.52.110-.130 (West 1988); W. VA. CODE §§ 61-3C-1 to -21 (1997); WIS. STAT. ANN. § 943.70 (West 1996); WYO. STAT. ANN. §§ 6-3-501 to -505 (Michie 1999).

[166] *See* Erich Luening, *Court papers: Smith Admits to Creating Melissa Virus*, CNET (visited Nov. 11, 1999) <http://news.cnet.com/news/0-1005-202-346448.html>.

the Melissa virus became the fastest-spreading virus in Internet history.[167] Recipients of the message containing the Melissa virus activated the virus by opening a Microsoft Word document sent as an e-mail attachment.[168] Upon opening the document, the virus re-sent itself and the triggering document to the first fifty addresses on the recipient's Microsoft Outlook e-mail list.[169] The document that was sent to the subsequent recipients contained the subject line "Important Message From [sender's name]".[170] Thus, since the attached document appeared to come from a trusted source, it is likely that most recipients opened the document with little suspicion that they were triggering the Melissa virus.

54. The FBI's National Infrastructure Protection Center ("NIPC") subsequently issued a warning to Internet users with respect to the operation and effect of the Melissa virus.[171] One graduate student noticed that the Melissa virus was similar to those written by a virus writer known as "VicodinES."[172] This information helped in tracking down its author, David L. Smith.[173] On April 2, 1999, the FBI and the New Jersey State Police arrested Smith for creating and disseminating the Melissa virus.[174] "Smith pleaded not guilty to [state] charges of interrupting public communication, conspiracy to commit the offense, and the attempt to commit the offense."[175] But in August 1999, Smith admitted to the authorities that he created the Melissa virus.[176] As of this writing, the outcome of this case is still pending, but if Smith is convicted on the state charges, he will face "a maximum of 40 years in prison and fines of [up to] $480,000."[177]

---

[167] *See FBI Press Room - 1999 - Congressional Statement, Melissa Macro Virus* (last modified Dec. 14, 1999) <http://www.fbi.gov./pressrm/congress/congress99/vatis1.htm> (quoting Steven M. White, an IBM researcher as saying that "'[b]ecause of the way Melissa virus spreads, it represents a new page in the history of viruses.'").

[168] *See id.*

[169] *See id.*

[170] *See id.*

[171] *See id.*

[172] Hacker Sitings and News, *How They Caught Him, Tracking the Hacker Who Hatched the Melissa Virus* (visited Nov. 11, 1999) <http://www.infowar.com/hacker/99/hack_041299a_j.shtml>.

[173] *See id.*

[174] *See* FBI Press Room, *supra* note 167; Luening, *supra* note 166.

[175] Luening, *supra* note 166.

[176] *See id.*

[177] *Id.*

55. It took experts several days to get the Melissa virus under control.[178] As a result, during a subsequent virus scare in the fall of 1999, the FBI's NIPC director Michael A. Vatis urged "[e]-mail users [to] exercise caution when reading their [e]-mail . . . and [to] bring unusual messages to the attention of their system administrator."[179]

56. Further, if Smith's employer made it possible for him to create and disseminate the Melissa virus onto the Internet by providing him with a computer with Internet access[180] and if it was foreseeable that Smith would use the Internet for personal use, his employer may face liability due to Smith's illegal online activity.[181]

c. Examples of Worms and Potential Employer Liability

57. A Cornell University graduate student, Robert Morris, began "[t]he largest [worm] incident in Internet history" on November 2, 1988, when he "unleashed a program that spawned copies of itself and spread throughout the network."[182] The worm quickly invaded between 2,000 and 6,000 computers, representing "between 3% and 10% of the total Internet at the time. The program also clogged the systems it hit, dialing virtually every computer it invaded."[183] System administrators had to disconnect systems from the Internet, or even shut them down, for several days, in order to repair the damage.[184]

58. Morris was convicted of violating the CFFA.[185] The Second Circuit held that when Morris released the computer "worm" onto the Internet that multiplied and caused computers at various educational, governmental and military institutions to "crash," Morris knowingly accessed and damaged "protected computers," and therefore

---

178 *See* FBI Press Room, *supra* note 167.

179 NIPC Alert, *Explorer Zip Worm* (last modified Oct. 21, 1999) <http://www.fbi.gov/nipc/zipworm.htm>. Information on detection and mitigation strategies can be obtained online from *CERT® (the Computer Emergency Response Team at Carnegie Mellon University)* (visited Oct. 6, 1999) <http://www.cert.org>.

180 *See generally supra* notes 54-62 (discussing employer liability rational based on the fact that the employer's job created the opportunity for the employee to commit the wrongful or illegal act).

181 *See generally supra* notes 51-64 (discussing when courts will hold an employer liable for its employee's foreseeable illegal acts).

182 DENNING, *supra* note 146, at 280.

183 *Id.*

184 *See id.*

185 *See* United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

violated the CFAA.[186] Consequently, Morris "was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision."[187]

59. Similar to the virus analysis, if an employer makes it possible for its employee to create and disseminate a worm into e-commerce by providing its employee with a computer that has Internet access;[188] and if it was foreseeable that the employee would use the Internet for personal use, the employer may face liability due to its employee's illegal online activity.[189]

60. Further, an employer may be held liable for its employee's act of creating and disseminating a virus or a worm into e-commerce if: (1) the act occurred within the employee's scope of employment, such as providing Internet access to its employees;[190] and (2) the employer knew or should have known that the employee was creating and disseminating a virus or a worm into e-commerce via the Internet at the workplace.[191]

4. Internet Gambling

61. Similar to the increase of e-mail and Internet usage in the workplace, "gambling"[192] is growing rapidly in the United States.[193] Over the last thirty years, the number of Americans that have gambled has increased substantially.[194] In 1998,

---

[186] *See id.* at 505, 511.

[187] *Id.* at 506.

[188] *See generally supra* notes 54-62 (discussing employer liability rational based on the fact that the employer's job created the opportunity for the employee to commit the wrongful or illegal act).

[189] *See generally supra* notes 51-64 (discussing when courts will hold an employer liable for its employee's illegal foreseeable acts).

[190] *See generally supra* Section II(B) (discussing what acts fall within the scope of the employee's employment).

[191] *See generally supra* notes 51-64 (discussing when courts will hold an employer liable for its employee's illegal foreseeable acts).

[192] Gambling under common law is defined "as any activity involving a bet, a prize and the element of chance." *Sports Fantasy or Felony?*, PRESS-ENTERPRISE, Apr. 4, 1998, at C1, *available in* 1998 WL 5679535.

[193] *See* Ante Z. Udovicic, *Special Report: Sports and Gambling a Good Mix? I Wouldn't Bet On It.*, 8 MARQ. SPORTS L.J. 401, 401 (1998); *see also* Fojut, *supra* note 18, at 155 (explaining that the gambling industry is easily bigger than the movie and music industries combined).

[194] *See* Udovicic, *supra* note 193, at 401. In the 1970s, approximately 60% of Americans gambled in some capacity while in the 1980s, approximately 80% of Americans gambled. *See id.* Commentators believed that by 1995, about 85% of Americans gambled. *See id.*

estimates were that Americans would wager at least $600 billion that year alone, or in other words, "$2,400 per man, woman and child."[195] Furthermore, it is estimated "that compulsive gambling affects about three percent of the population (or approximately nine million people), and an estimated eighty percent of the general population has gambled to some degree."[196]

62. As one might expect, gambling has been declared an undesirable activity.[197] Several states have exercised their Tenth Amendment police power by prohibiting gambling in order to protect the health and safety of their citizens.[198] Moreover, under federal law, the government regulates gambling through the Commerce Clause.[199] However, despite state and federal effort, gambling remains a part of the American culture and continues to grow.[200] A factor contributing to this growth is the introduction of Internet casino gambling in 1995.[201] Presently, there are hundreds of gambling Websites operating on the Internet.[202] Not only can the Internet gambler

---

[195] Steven Crist, *All Bets Are Off*, SPORTS ILLUSTRATED, Jan. 26, 1998, at 82, *available in* 1998 WL 8979198.

[196] Udovicic, *supra* note 193, at 401-02; *see also* Crist, *supra* note 195 (noting that Tom Grey, director of the National Coalition Against Legalized Gambling estimates that compulsive gambling affects 5% of the American population); *see also* Fojut, *supra* note 18, at 161-62 (explaining that children are susceptible to becoming addicted to Internet gambling). Many believe that Internet gambling could increase the percentage of the population who will become compulsive gamblers because of the ease of access to gambling on the Internet. *See* Crist, *supra* note 195. Experts believe that if Internet gambling is not barred, then this group will increase dramatically and a large number of these gambling addicts will gamble themselves into bankruptcy. *See id.*

[197] *See* Champion v. Ames, 188 U.S. 321, 357 (1902) (holding that Congress has the power to regulate inherently evil objects such as lottery tickets from being transported through interstate commerce).

[198] *See* State v. Strawberries, Inc., 473 N.W.2d 428, 437 (Neb. 1991) (noting that states' prohibition of gambling is a legitimate exercise of their police power).

[199] *See generally* United States v. Zizzo, 120 F.3d 1338, 1350 (7th Cir. 1997) (noting that "[u]nder the Commerce Clause, Congress has the power to regulate . . . activities that substantially affect interstate commerce. . . . Congress [has] found that illegal gambling fills the coffers of organized crime, which in turn has a substantial effect on interstate commerce.").

[200] *See* Fred Faust, *Gambling Commission Considers Net Casinos*, ST. LOUIS POST-DISPATCH, May 25, 1998, at 2, *available in* Westlaw, SLPD FILE; *see also* Udovicic, *supra* note 193, at 404 (noting that gambling has continued to grow in the 1990s).

[201] *See* Faust, *supra* note 200, at 2; *see also* Udovicic, *supra* note 193, at 413 (discussing how participation in gambling has become much more convenient since the introduction of the Internet).

[202] *See* Place Your Bet, *Top 100 Gambling and Casino Sites in the World* (visited Mar. 15, 2000) <http://www.placeyourbet.net/topsites/main.html> (providing links to over 200 Internet gambling sites); *see also* Crist, *supra* note 195 (noting that one Internet gambling site received 250 bets per second during the interval between the 1998 AFC and NFC championship games); Fojut, *supra* note 18, at 158 ("Several dozen gambling sites are currently operated on the world wide web.").

participate in all the traditional forms of gambling (e.g., casino wagering, sports wagering, horse and dog wagering and lotteries), but the Internet gambler can also participate in non-traditional forms of gambling such as political elections and armed conflict wagering.[203]

63. One explanation for the rapid growth of Internet gambling is its ease – just a few clicks on a user's mouse, and one can gamble at a 'cyber casino.'[204] First, the gambler conducts a search on the Internet for a gambling site.[205] Once linked to a gambling site, the gambler opens an account with the site by either a credit card, cash advance, bank-wire transfer, bank check or money order.[206] The account is opened, and the gambling begins.[207] Generally, winnings are delivered to the gambler via credit to the gambler's account.[208] Otherwise the winnings are mailed or delivered to the gambler by a courier.[209]

64. Experts anticipate that Internet gambling will "'be a multi-billion dollar industry within [the next] five years.'"[210] In 1996, it was estimated that Americans wagered between $100 million and $200 million over the Internet.[211] Currently, the United States government estimates that at least fifteen million Americans have lost approximately $1 billion in gambling on the Internet.[212] Moreover, statistical experts

---

[203] *See* Crist, *supra* note 195 (explaining unique events that some individuals wagered on and how easy it is to place a bet on the Internet).

[204] *See* Nicholas Robbins, Note, *Baby Needs A New Pair of Cybershoes: The Legality of Casino Gambling on the Internet*, 2 B.U. J. SCI. & TECH. L. 7, ¶ 2 (1996).

[205] *See* Crist, *supra* note 195.

[206] *See id.*

[207] *See id.*

[208] *See id.*

[209] *See id.*

[210] Udovicic, *supra* note 193, at 413; *see also* Faust, *supra* note 200, at 2 (stating that the National Gambling Impact Study Commission expects "Internet casino revenues to range from $1.5 billion to $10 billion by [the year] 2000.").

[211] *See* Fojut, *supra* note 18, at 159; Crist, *supra* note 195 (noting that Internet gambling bets were expected to exceed $600 million in 1998).

[212] *See* David E. Rovella, *Suits Challenge Net Bet Debt: Plaintiffs Say That Laws Ban Collection Via Credit Cards*, LAW NEWS NETWORK (last modified Aug. 11, 1999) <http://www.lawnewsnet.com/stories/A3745-1999Jul23.html>; *see also* Dirk Johnson, *In a Legal Gray Area, Blackjack is a Click Away*, NEW YORK TIMES – TECH. (visited Nov. 11, 1999) <http://www.nytimes.com/library/tech/99/08/biztech/technology/22john.html>; Wendy R. Leibowitz, *Senate Bans Most 'Net Gambling; Many Bet on Poor Enforcement*, NAT'L L.J., Aug. 10, 1998, at B6 ("The Justice Department estimates that approximately $600 million is spent gambling online.").

predict that "Internet gambling will generate approximately $50 billion in revenue by the year 2000"[213] and possibly over $200 billion by the year 2005.[214]

65. In addressing Internet gambling under the respondeat superior doctrine, an employer may be held liable under both state and federal law when its employee wagers online.[215] In defining when the employer may be held liable for its employee's use of the Internet to gamble at the workplace, it is necessary to first examine the behavior that constitutes illegal Internet gambling.

a. Employer Liability Based On Federal Law

66. Surprisingly, under federal law, the individual act of Internet gambling is not illegal.[216] Three federal statutes regulate, but do not criminalize, the individual act of Internet gambling. Under Section 1084 of the Interstate Wire Act, it is illegal to "engage in the business of betting" and to "knowingly use a wire communication facility" to transmit bets or wagering information in interstate or foreign commerce.[217]

---

[213] Fojut, *supra* note 18, at 159.

[214] *See id.*

[215] *See generally* Section II(B) (explaining the modern theory of respondeat superior).

[216] *See generally* Udovicic, *supra* note 193, at 413 n.74 (noting that proposed amendments to the Wire Communications Act would extend its coverage to Internet gambling).

[217] Interstate Wire Act, 18 U.S.C. § 1084 (1994). The relevant portion of the statute provides:

> (a) Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.
> (b) Nothing in this section shall be construed to prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting event or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State or foreign country where betting on that sporting event or contest is legal into a State or foreign country in which such betting is legal.
> . . .
> (d) When any common carrier, subject to the jurisdiction of the Federal Communications Commission, is notified in writing by a … law enforcement agency … that any facility furnished by it is being used or will be used for the purpose of transmitting or receiving gambling information in interstate or foreign commerce in violation of Federal, State, or local law, it shall discontinue . . . the leasing, furnishing, or maintaining of such facility, after reasonable notice to the subscriber, but no damages, penalty or forfeiture, civil or criminal, shall be found against any common carrier for any act done in compliance with any notice received from a law enforcement agency.

Id. § 1084(a), (b), (d).

Despite the definition of "wire communication," which arguably includes the Internet,[218] the Act does not make it a federal crime for an individual gambler, who is not in the "business of betting," to gamble on the Internet.[219] This statute was designed to prevent "bookies" from accepting bets or wagers on a telephone.[220] Thus, a "wireless" communication by an individual to transmit bets or wagering information in interstate or foreign commerce is not illegal under the Act.[221]

67. Under Section 1952 of the Travel Act, it is illegal to use an interstate facility to operate or facilitate a gambling enterprise.[222] Congress drafted the Travel Act broadly to prohibit the use of channels of interstate and foreign commerce for the furtherance of criminal activity.[223] However, the Travel Act has been interpreted to apply only to those engaged in criminal enterprises, and not individuals.[224] Therefore, the Travel Act does not cover the individual act of Internet gambling.

68. Finally, under Section 1955 of the Organized Crime Control Act, it is illegal to conduct certain gambling businesses.[225] Under this Act, any person convicted of

---

[218] A "wire communication facility" is defined as "any and all instrumentalities, personnel, and services (among other things, the receipt, forwarding, or delivery of communications) used or useful in the transmission of writings, signs, pictures, and sounds of all kinds by aid of wire, cable or other like connection between the points of origin and reception of such transmission." 18 U.S.C. § 1081 (1994). However, some commentators argue that "the Interstate Wire Act did not specifically identify the mode of transmission of information and communication that represents the Internet as a prohibited means of transmission." Fojut, *supra* note 18, at 161.

[219] *See* 18 U.S.C. § 1084(a).

[220] *See* Montpas, *supra* note 6, at 180-81.

[221] *See* 18 U.S.C. § 1084(a).

[222] Travel Act, 18 U.S.C. § 1952 (a)-(b) (1994). The Act sanctions:

> (a) Whoever travels in interstate or foreign commerce or uses the mail or any facility in interstate or foreign commerce, with intent to-
> (1) distribute the proceeds of any unlawful activity; or
> (2) commit any crime of violence to further any unlawful activity; or
> otherwise promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on, of any unlawful activity, and thereafter performs or attempts to perform . . . [any of the acts described in (1), (2), and (3)].
> (b) As used in this section (i) "unlawful activity" means (1) any business enterprise involving gambling. . . .

Id.

[223] *See* Erlenbaugh v. United States, 409 U.S. 239, 246-47 (1972).

[224] 18 U.S.C. § 1952 (a)-(b); United States v. Roberson, 6 F.3d 1088, 1094 (5th Cir. 1993) ("The purpose of the Act is clear . . . . It is not aimed at individual substantive offenses.").

[225] Organized Crime Control Act, 18 U.S.C. § 1955 (1994).

owning or operating an "illegal gambling business" is subjected to a fine, imprisonment for five years, or both.[226] Again, however, this Act does not regulate the individual Internet gambler, because the Supreme Court has held that this Act may only be used to prosecute Internet gambling businesses.[227]

69. Recently, Senator Jon Kyl of Arizona and Congressman Bob Goodlatte of Virginia introduced similar bills in both the United States Senate and House of Representatives that seek to prohibit online gambling businesses.[228] Both bills include extensive sets of provisions dealing with interactive computer services, such as American Online and Web hosting companies, seeking to protect interactive computer services from liability for providing the communication for others to gamble online.[229] However, the current versions of these two bills do not penalize the individual online gambler.

70. Therefore, under federal law, an employer may be held vicariously liable for its employee's online gambling only if: (1) the employee is operating a "bookie" operation; (2) the bookie activity occurred within the employee's scope of employment; and (3) the wrongful act was known or should have been known by the employer. However, as of this Comment, the individual act of online gambling is not punishable under federal law.[230] Consequently, in defining when an employer may be held liable

---

226 *Id*. § 1955(a).

227 *See* Sanabria v. United States, 437 U.S. 54, 70 n.26 (1978) ("Numerous cases have recognized that . . . [Section] 1955 . . . proscribes any degree of participation in an illegal gambling business, except participation as a mere bettor."); *see also* United States v. Pinelli, 890 F.2d 1461, 1470-71 (10th Cir. 1989).

228 *See* Internet Gambling Prohibition Act of 1999, S. 692, 106th Cong. (1999); Internet Gambling Prohibition Act of 1999, H.R. 3125, 106th Cong. (1999); *Bill Summary & Status* (visited Mar. 12, 2000) <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN00692:@@@X>.

229 *See* Internet Gambling Prohibition Act of 1999, S. 692, 106th Cong. (1999) (proposing 18 U.S.C. § 1085(d)); Internet Gambling Prohibition Act of 1999, H.R. 3125, 106th Cong. (1999) (proposing 18 U.S.C. § 1085(d)); *Yahoo! Government: U.S. Government: Legislative Branch: Senate: Senators* (visited Mar. 12, 2000) <http://dir.yahoo.com/Government/U_S__Government/Legislative_Branch/Senate/Senators/>; *Yahoo! Government: U.S. Government: Legislative Branch: House of Representatives: Representatives* (visited Mar. 12, 2000) <http://dir.yahoo.com/Government/U_S__Government/Legislative_Branch/House_of_Representatives/Representatives/>.

230 There are additional federal laws that govern gambling. For example, the Federal Aiding and Abetting Statute punishes anyone who "commits an offense against the United States or aids, abets . . . or procures its commission . . . ." 18 U.S.C. § 2(a) (1994). The Interstate Transportation of Wagering Paraphernalia Act imposes criminal penalties against any person who "knowingly carries or sends in interstate or foreign commerce any . . . paraphernalia . . . or other device used . . . or designed for use" in illegal gambling. 18 U.S.C. § 1953(a) (1994). The Professional and Amateur Sports Protection Act provides that no person may "sponsor, operate, advertise, or promote . . . [a] betting, gambling, or wagering scheme based . . . on one or more competitive games in which

for its employee's criminal act of Internet gambling, it is necessary to examine state law.

b. Employer Liability Based On State Law

71. Generally, gambling is regulated through state law.[231] Indeed, "[e]ach state determines whether gambling will be permitted within its boundaries -- and, if it is permitted, what specific forms of gambling will be allowed."[232] Currently, Hawaii and Utah are the only states that prohibit all forms of gambling.[233] All other states permit gambling to some degree (e.g., casinos, horse wagering, dog wagering and lotteries).[234] As of this writing, the majority of states have laws which could be construed to ban Internet gambling. These states include Alabama,[235] Arizona,[236] California,[237]

---

amateur or professional athletes participate . . . ." 28 U.S.C. § 3702(2) (1994).

Furthermore, under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), an employer may also be penalized for its employee's illegal online gambling activity if it constitutes a "racketeering activity". 18 U.S.C. § 1961 *et seq*. (1994). Under RICO, racketeering activity includes activities by a person that represents a pattern of "racketeering activity" or collections of unlawful debt, and that are indictable under, inter alia, the Wire Act and the Travel Act. *See id*. §§ 1961-62. Thus, if an employee operates an online gambling enterprise using the employer's technology while at the workplace, the employer may also be penalized under RICO.

231 *See* U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."); *see also* Thomas v. Bible, 694 F. Supp. 750, 760 (D. Nev. 1988), *aff'd*, 896 F.2d 555 (9th Cir. 1990); *see also* State v. Rosenthal, 559 P.2d 830, 836 (Nev. 1977) ("We view gaming as a matter reserved to the states within the meaning of the Tenth Amendment to the United States Constitution."); Crist, *supra* note 195 (explaining that "gambling regulation has traditionally been a state rather than a federal function."); Faust, *supra* note 200, at 2; Fojut, *supra* note 18, at 155.

232 Fojut, *supra* note 18, at 155; *see also* Crist, *supra* note 195 (noting that gambling is mostly prohibited in the United States, "'and where it is not, it is highly regulated.'").

233 *See* Fojut, *supra* note 18, at 155.

234 *See id*.; Montpas, *supra* note 6, at 165-67 (discussing the history of state regulation of gambling). Thirteen states have riverboat or casino gambling. *See* Representative Bill McCollum, *Opening Statement of Chairman McCollum Before the House Judiciary Crime Subcommittee on Internet Gambling*, Feb. 4, 1998, *available in* 1998 WL 8991665. Only Nevada has sports gambling. *See* Claire Ann Koegler, *Here Come the Cybercops 3: Betting on the Net*, 22 NOVA L. REV. 545, 551-52 (1998). "Thirty-six states and the District of Columbia now have state lotteries . . . ." H.R. REP. NO. 104-440, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1192, 1193. "These figures neither include gambling on Native American lands nor cruises to nowhere but international waters for the purpose of gambling." Koegler, *supra* note 234, at 552.

235 *See* ALA. CODE § 13A-12-21 (1999) ("A person commits the crime of simple gambling if he knowingly advances or profits from unlawful gambling activity as a player.").

236 *See* ARIZ. REV. STAT. § 13-3307 (1989) (penalizing any person who "knowingly possesses any book, writing, paper, instrument, article, electronically-produced data, computer software and programs,

Colorado,[238] Connecticut,[239] Delaware,[240] Hawaii,[241] Illinois,[242] Kansas,[243] Louisiana,[244] Massachusetts,[245] Minnesota,[246] Missouri,[247] Nebraska,[248] Nevada,[249] North Carolina,[250]

---

discs, tapes or other tangible or intangible method of recording information knowing or having reason to know that it arises out of, or was made in connection with, gambling in violation of this chapter."). Arizona law additionally provides that:

> no person may engage for a fee, property, salary or reward in the business of accepting, recording or registering any bet, purported bet, wager, or purported wager or engage for a fee, property, salary or reward in the business of selling wagering pools or purported wagering pools with respect to the result or purported result of any race, sporting event, contest or other game of skill or chance or any other unknown or contingent future event or occurrence whatsoever.

ARIZ. REV. STAT. § 13-3305 (1989). A 1998 bill would have amended § 13-3305 to prohibit the use of communications facilities to send or receive information regarding wagering pools, but the bill did not pass. *See* H.B. 2367, 43d Leg., 2d Reg. Sess. (Ariz. 1998), *available in* ALIS Online, *HB2367 – 432R – I Ver – Title: Internet Gambling* (last modified Feb. 10, 1998) <http://www.azleg.state.az.us/legtext/43leg/2r/bills/hb2367p.htm>; *see also* ARIZ. REV. STAT. § 13-3305 (1999) (showing that the current version of the statute does not include the proposed changes in H.B. 2367); ALIS Online, *HB2367 – 432R – Status – Title: Internet Gambling* (visited Mar. 14, 2000) http://www.azleg.state.az.us/cgi-bin/waisgate?WAISaction=retrieve&WAISdocID=3833225272+56+0+0> (showing that the bill's final status was a second reading on January 19, 1998).

[237] *See* CAL. PENAL CODE § 337i (West 1999). Under California law, it is illegal to transmit "information as to wagers" over the telephone or "any means whatsoever . . . ." *Id.* Such means could presumably include the Internet.

[238] *See* COLO. REV. STAT. §§ 18-10-102, 18-10-106 (1999) (penalizing persons that transmit or receive gambling information, e.g., a "communication with respect to any wager made in the course of, and any information intended to be used for, professional gambling.").

[239] *See* CONN. GEN. STAT. ANN. § 53-278c (West 1994) (providing that "[a]ll gambling devices are common nuisances and . . . are subject to seizure . . . ."); 1998 Conn. Pub. Acts 220 (deeming the use of any real property to transmit gambling information a nuisance).

[240] *See* DEL. CODE ANN. tit. 11, § 1411 (1995) (sanctioning a person who "knowingly uses a private wire in disseminating or receiving information in furtherance of gambling or for gambling purposes . . . .").

[241] *See* HAW. REV. STAT. ANN. § 712-1223 (Michie 1999) (declaring all gambling activity illegal in the state of Hawaii).

[242] *See* 720 ILL. COMP. STAT. ANN. 5/28-1 *et seq.* (West 1993) (prohibiting the transmission of "information as to wagers, . . . by telephone, telegraph, radio, semaphore, or similar means . . . ."); *see also* Rovella, *supra* note 212 (explaining that Illinois specifically bans Internet gambling); S.B 1687, 90th Leg., Gen. Ass. (Ill. 1997-98), *available in State of Illinois: 90th General Assembly: Legislation* (last modified Feb. 28, 2000) <http://www.legis.state.il.us/legisnet/legisnet90/sbgroups/sb/900sb1687lv.html> (seeking to create the Internet Gambling Limitation Act which would make using the Internet to conduct or assist in gambling a Class A misdemeanor). Bill 1687, however, died in the Senate Rules Committee. *See* Status of SB 1687 (visited Mar. 14, 2000)

<http://www.legis.state.il.us/scripts/imstran.exe?LIBSINPWSB1687>.

[243] *See* KAN. STAT. ANN. § 21-4308 (1995) (prohibiting the knowing installation of "communication facilities . . . that . . . [are] be[ing] used principally for the purpose of transmitting information to be used in making or settling bets . . . .").

[244] *See* LA. REV. STAT. ANN. § 90.3 (West 1986 & Supp. 2000); H.B. 2480, Reg. Sess. (La. 1997) (prohibiting anyone from conducting or assisting in conducting a business that involves Internet gambling); *see also* Rovella, *supra* note 212 (explaining that Louisiana specifically bans Internet gambling).

[245] *See* MASS. GEN. LAWS ANN. ch. 271, § 17A (West 1990). Under Massachusetts law, it is illegal to use the telephone to place a bet or wager. *See id.*

[246] *See* MINN. STAT. ANN. §§ 609.75 (2)-(3), 609.755 (1) (West 1987 & Supp. 1999) (prohibiting Minnesota residents from placing bets through gambling organizations, arguably including Internet based ones); *see also* Complaint, Introduction, ¶ 2, State v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (Minn. Ct. App. 1997) (No. C6-95-72227) (alleging the State's jurisdiction over Internet gambling under its consumer protection laws, which prohibit deceptive trade practices, false advertising, and consumer fraud); Dan Goodin, *Online Wagering: Place Your Bet On the Internet*, LAS VEGAS REV. J., July 23, 1995, at 1C, *available in* 1995 WL 5795946. Furthermore, the Minnesota Attorney General has stated that:

> [p]ersons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws.
> . . .
> Gambling appears to be an especially prominent aspect of criminal activity on the Internet. There are a number of services outside of Minnesota that offer Minnesota residents the opportunity to place bets on sporting events, purchase lottery tickets, and participate in simulated casino games. These services are illegal in Minnesota.

Minnesota Attorney General, *Warning to All Internet Users and Providers* (last modified Sept. 18, 1998) <http://www.ag.state.mn.us/home/consumer/consumernews/onlinescams/memo.html>.

[247] *See* MO. ANN. STAT. §§ 572.010-030 (West 1995) (prohibiting gambling activity). *See generally* State *ex rel.* Nixon v. Interactive Gaming & Communications Corp., CV 97-7808 (Mo. Cir. Ct. 1997), *available in* Bureau of National Affairs, Inc., *EPLR: Missouri v. Interactive Gaming* (visited July 3, 1999) <http://www.bna.com/e-law/cases/intergame.html>. In *Interactive Gaming*, the court held that Internet gambling companies may not represent that Internet gambling services are legal in the state of Missouri. *See id.* The court reasoned that such representation violated the Missouri Merchandising Practices Act, MO. ANN. STAT. § 407.020 (West Supp. 2000), which prohibits any misrepresentation "in connection with the sale or advertisement of any merchandise in trade or commerce . . . ." *Id.*

[248] *See* NEB. REV. STAT. § 28-1101(5), 1107 (1995) (prohibiting the "possession of a gambling device, . . ." defined to include "any device, . . . that is used or usable for engaging in gambling . . . .").

[249] *See* NEV. REV. STAT. §§ 465.091-.092 (1999) (showing that Nevada specifically prohibits gambling "through any medium of communication," which is defined to include the Internet); *see also* Rovella, *supra* note 212.

Pennsylvania,[251] Texas[252] and Utah,[253] who have, or arguably have, prohibited the individual act of Internet gambling. California,[254] Hawaii,[255] Indiana,[256] and New York[257]

---

[250] *See* N.C. GEN. STAT. § 14-292 (Michie 1999). North Carolina law arguably is broad enough to prohibit Internet gambling by both individuals and casinos:

> Except as provided in Part 2 of this Article [which addresses bingo and raffles], any person or organization that operates any game of chance or any person who plays at or bets on any game of chance at which any money, property or other thing of value is bet, whether the same be in stake or not, shall be guilty of a Class 2 misdemeanor.

Id.

North Carolina law also prohibits gambling in a place of public entertainment. *See* N.C. GEN. STAT. § 14-293. Thus, an "Internet café" could be held criminally liable if it is aware that one or more of its customers use its facilities to gamble over the Internet.

However, much of North Carolina's gambling law is antiquated with respect to the Internet. Most of the sections are targeted at the use of various gambling devices. *See, e.g.*, N.C. GEN. STAT. § 14-294 (regarding "faro banks and tables"); *id*. § 14-295 (prohibiting the "[k]eeping [of] gaming tables, illegal punch-boards or slot machines . . ."); *id*. § 14-297 (prohibiting the "[a]llowing [of] gaming tables, illegal punch-boards or slot machines on premises"); *id*. §§ 14-298-300 (providing for seizure, disposition, and destruction of "[g]aming tables, illegal punchboards and slot machines"); *id*. §§ 14-301 to 302 (providing separate offenses for operation and possession of slot machines, punch boards, vending machines, and other gambling devices); *id*. § 14-304 (prohibiting the "[m]anufacture, sale, etc., of slot machines and devices").

"Faro banks" and "punch-boards" are not specifically defined by the code, but "slot machine or device" is defined narrowly as a machine in which a coin or slug is inserted to make it operate, so that the user may receive something of value in return. *See id*. § 14-306. Further, it must be "designed and manufactured primarily for use in connection with gambling and which machine or device is classified by the United States as requiring a federal gaming device tax stamp under applicable provisions of the Internal Revenue Code." N.C. GEN. STAT. § 14-306.

Hence, an Internet gambler's computer cannot be classified as a gambling device within North Carolina law, and a person's use of her computer to gamble online falls outside of all of the sections listed above other than § 14-292.

Unlike the specific prohibitions on gambling, North Carolina's law addressing advertising lotteries is effective against Internet lotteries:

> Except in connection with a lawful raffle as provided in Part 2 of this Article, if anyone . . . in any . . . way, advertise[s] or publish[es] an account of a lottery, whether within or without this State, stating how, when or where the same is to be or has been drawn, or what are the prizes therein or any of them, or the price of a ticket or any share or interest therein, or where or how it may be obtained, he shall be guilty of a Class 2 misdemeanor.

Id. § 14-289. Thus, it appears that Internet lotteries are illegal under North Carolina law.

[251] *See* PA. STAT. ANN. tit. 66, § 2902 (West 1979) (prohibiting any public utility from assisting any person in using a wire communication to distribute information in furtherance of gambling or for gambling purposes).

[252] *See* TEX. CIV. PRAC. & REM. CODE ANN. § 125.041 (West 1997) (deeming any "gambling, gambling promotion or communication of gambling information" a public nuisance if occurring at some place "on a regular basis"); *see also* Rovella, *supra* note 212 (explaining that Texas specifically bans Internet gambling).

[253] *See* UTAH CONST. art. VI, § 27 (providing that the state of Utah may not authorize lotteries).

[254] Some California bills from the 1997-98 legislative sessions showed an intent to reach Internet gambling. *See* A.B. 2655, Gen. Ass., Reg. Sess. (Cal. 1997-98), *available in AB 2655 Assembly Bill – INTRODUCED* (last modified Nov. 8, 1998) <http://www.leginfo.ca.gov/pub/97-98/bill/asm/ab_2651-2700/ab_2655_bill_19980223_introduced.html> (stating the intent of the Legislature to regulate gambling conducted in the State of California using any medium of communication, defined to include the Internet, in a bill to be codified in the Business and Professions Code as Section 19801.3). A.B. 2655, however, was not passed. *See AB 2655 Assembly Bill – Status* (last modified Nov. 8, 1998) <http://www.leginfo.ca.gov/pub/97-98/bill/asm/ab_2651-2700/ab_2655_bill_status.html>; CAL. BUS. & PROF. CODE § 19801 (West 1997 & Supp. 2000) (showing that the current version of the California statute does not include the proposed section).

Moreover, California Senator Leslie introduced a bill which would amend § 337j of the California Penal Code, to read: "Every person who knowingly uses an interactive computer service or system to engage in gaming, to transmit bets or wagers, or to receive money or credit as a result of gaming or placing bets or wagers, is guilty of a misdemeanor." *See* S. 777, Gen. Ass., Reg. Sess. (Cal. 1997-98) (amending CAL. PENAL CODE § 337j(a)), *available in SB 777 Senate Bill – AMENDED* (last modified Nov. 8, 1998) <http://www.leginfo.ca.gov/pub/97-98/bill/sen/sb_0751-0800/sb_777_bill_19970501_amended_sen.html>. This bill, however, was not enacted. *See SB 777 Senate Bill – Status* (last modified Nov. 8, 1998) <http://www.leginfo.ca.gov/pub/97-98/bill/sen/sb_0751-0800/sb_777_bill_19970501_amended_sen.html> (showing that the final action on S.B. 777 was that it was "[r]eturned to Secretary of Senate pursuant to Joint Rule 56"); CAL. PENAL CODE § 337j (West 1999) (showing that these changes are not reflected in the current statute).

[255] *See* H.C.R. 150, 19th Leg., Reg. Sess. (Haw. 1997) (urging Congress to enact legislation banning gambling on the Internet). As noted earlier, Hawaii bans all types of gambling. *See id.*

[256] *See* H.B. 1095, 111th Leg., 2d Reg. Sess. (Ind. 2000), *available in Introduced Version, House Bill 1095* (visited Mar. 14, 2000) <http://www.state.in.us/legislative/bills/2000/IN/IN1095.1.html>. Currently pending Indiana House Bill 1095 provides that: (1) "Internet gambling [is] a Class B misdemeanor;" (2) "providing gambling through the Internet [is] a Class D felony;" (3) "an interactive computer service [shall] . . . discontinue its service if it is notified by a law enforcement agency that the service is being used to promote professional gambling;" and (4) "[r]equires an interactive computer service to block access to a site used to promote professional gambling." *Id.* Thus, an employer "who knowingly or intentionally [allows an employee to] engage[] in [gambling] by means of the World Wide Web[] commits professional gambling, a Class D felony." *Id.*

[257] *See* A.B. 7818, 220th Leg., Reg. Sess. (N.Y. 1997). Bill 7818 would require persons, firms, corporations or other legal entities that provide gambling or wagering services over the Internet to post a bond with the State Racing and Wagering Board, while carving out an exception for those entities offering horse race betting only. *See id.*

Currently pending Bill 917 would provide that:

> any offense defined in this article which consists of the commission of acts involving the use of any computer communication system or electronic data storage medium allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to advance or profit from gambling activity is no less criminal because one or more of such acts is committed without the state and is not violative of the laws of the jurisdiction in which it was so committed.

S. 917, 222d Leg., Reg. Sess. (N.Y. 1999), *available in New York State Assembly –Bill S00917 Text* (visited Mar. 12, 2000) <http://www.assembly.state.ny.us/cgi-bin/showtext?billnum=S00917>.

Currently pending Bill 918 would provide that:

> any offense defined in this article which consists of the commission of acts involving the use of any computer communication system or electronic data storage medium allowing the

are just a few of the many states that are currently in the process of reforming their laws to explicitly prohibit the individual act of Internet gambling.

72. Thus, many states support the view that Internet gambling is an act warranting criminal sanctions.[258]

c. Examples of Online Gambling Conduct By Employees

73. Employers that provide employees with Internet access to conduct business also provide employees the opportunity to gamble on the Internet.[259] As explained earlier, the Supreme Court has acknowledged that the employer owns the communication equipment used at work, and it is the employer's business that is being conducted on this equipment.[260] Because this equipment may also allow the employee the opportunity to gamble, some courts may hold the employee's act of Internet

---

> input, output, examination or transfer, or computer data or computer programs from one computer to another, to disseminate access to gambling to a minor is no less criminal because one or more of such acts is committed without the state and is not violative of the laws of the jurisdiction in which it was so committed.

S. 918, 222d Leg., Reg. Sess. (N.Y. 1999), *available in New York State Assembly –Bill S00918 Text* (visited Mar. 12, 2000) <http://www.assembly.state.ny.us/cgi-bin/showbill?billnum=S00918>.

[258] A recent Louisiana statute has clearly stated this view:

> [A]ffording [the] opportunity for the fullest development of the individual and promoting the health, safety, education, and welfare of the people, including the children of this state who are our most precious and valuable resource, [the legislature] finds that the state has a compelling interest in protecting its citizens and children from certain activities and influences which can result in irreparable harm. The legislature has expressed its intent to develop a controlled well-regulated gaming industry. The legislation is also charged with the responsibility of protecting and assisting its citizens who suffer from compulsive or problem gaming behavior which can result from the increased availability of legalized gaming activities. . . . The legislature recognizes and encourages the beneficial effects computers, computer programming, and use of the Internet resources have had on the children of the state of Louisiana by expanding their educational horizons. The legislature further recognizes that it has an obligation and responsibility to protect its citizens, and in particular its youngest citizens, from the pervasive nature of gambling which can occur via the Internet and the use of computers connected to the Internet.

LA. REV. STAT. ANN. § 90.3 (West 1986 and Supp. 2000). This statute was added by a 1997 bill. *See* H.B. 2480, *available in 1997 Regular Session – Instrument Information* (visited Mar. 12, 2000) <http://www2.legis.state.la.us/bills97/avail_docs.asp?insttype=HB&billid=2480>.

[259] *See* Davidson, *supra* note 9, at 179 (noting that "courts impose respondeat superior liability on a blameless employer because the employee's job created the opportunity for the employee to commit the tort . . . .").

[260] *See supra* note 83 and accompanying text.

gambling to fall within the employee's scope of employment.[261] Furthermore, if the employer is located in a state where the individual act of Internet gambling is illegal, the employer may be held liable for its employee's criminal act of Internet gambling.[262] A state will likely have personal jurisdiction over a non-resident employer through its long-arm statute.[263]

74. Although there is no case law on point, a notable case recently settled in the state of California. In this case, defendant Haines lost over $70,000 while using her Providian National Bank credit card to gamble on the Internet.[264] When Providian sued the defendant for not paying her credit card bills, the defendant filed a counterclaim against Providian, as well as MasterCard and VISA, claiming that, because online gambling is illegal in California, credit card companies should be barred from collecting gambling debts owed by a California resident.[265] Haines reached a

---

261 *See* KEETON ET AL., *supra* note 54, § 69, at 499. Furthermore, an employer may not be relieved of its liability for its employee's action merely because the act was also punishable as a crime. *See* Panama R. Co. v. Toppin, 252 U.S. 308, 311 (1920) (interpreting Panamanian law); Collazo v. John W. Campbell Farms, Inc., 213 F.2d 255, 258 (5th Cir. 1954) (interpreting Florida law to extend liability to servant's criminal actions done "in the interest of the business of the employer."); Great S. Lumber Co. v. Williams, 17 F.2d 468, 471 (5th Cir. 1927) ("An employer is liable for . . . [criminal acts] committed while he is engaged in acts within his function or the scope of his authority . . . ."). *But see* Gibbs v. Air Canada, 810 F.2d 1529, 1532-33 (11th Cir. 1987); Hargrove v. Tree of Life Christian Day Care Ctr., 699 So. 2d 1242, 1246-47 (Ala. 1997) (relieving an employer from liability because a kidnapping constituted a gross deviation from employer's business); Roberson v. Allied Foundry & Mach. Co., 447 So. 2d 720, 723 (Ala. 1984); Collins v. Alabama G.S.R. Co., 16 So. 140, 142 (Ala. 1894).

262 *See* RESTATEMENT (SECOND) OF AGENCY § 231 cmt. a (1958). If the employer can reasonably anticipate that an employee may commit an act within the scope of the employee's employment, then the employer may be held liable for its employee's act. *See id.*

263 *See* State *ex rel.* Humphrey v. Granite Gate Resorts, Inc., 568 N.W.2d 715, 721 (Minn. Ct. App. 1997), *aff'd*, 576 N.W.2d 747 (Minn. 1998). The court held a non-resident defendant subject to personal jurisdiction in Minnesota based on Internet advertisements for an up-coming Internet gambling service. *See id.* at 721. The court reasoned that the placement of Internet advertisements indicated the non-resident defendant's "clear intent to solicit business from markets that includ[ed] Minnesota . . . ." *Id.*

In *People of New York v. World Interactive Gaming Corp.*, a New York appellate court held that the New York Attorney General had personal jurisdiction over an Internet gaming company. No. 404428/98, 1999 WL 591995, at *4 (N.Y. App. Div. July 22, 1999); *see also* New York State Attorney General Press Releases, *Spitzer Wins Precedent-Setting Internet Casino Gambling Case* (visited Nov. 11, 1999) <http://www.oag.state.ny.us/press/1999/jul/jul26a_99.html>. The court reasoned that the company's Website created a "virtual casino within the user's computer terminal" in New York State. *World Interactive Gaming Corp.*, at *7.

264 *See Suit Against Credit Card Companies Seeks to Nullify $70,000 Internet Gambling Debt*, 4 Bank & Lender Liab. Litig. Rep. (Andrews Pubs., Inc.) (Oct. 21, 1998), available in WESTLAW, ANBLLLR File; Courtney Macavinta, *Providian May Bar Customers from Net Gambling*, CNET (visited Nov. 3, 1999) <http://news.cnet.com/news/0-1005-202-923070.html>.

265 *See id.*

settlement with VISA whereby VISA agreed to seek reimbursement from the gambling Websites.[266]

75. Assume, however, that the defendant in the Providian National Bank situation made online wagers using her employer's computer while taking a reasonable break from her work-related duties. The state of California could prosecute the defendant's employer for her online gambling because Internet gambling is illegal in the state of California.[267] If the court applies the modern trend of employer liability, the state of California will succeed. Her employer made it possible for her to make the online wagers by providing her a computer with Internet access.[268] It was foreseeable that an employee may use the Internet for personal use.[269] Consequently, under the modern trend of employer liability, the defendant's online gambling occurred within the scope of her employment and liability may be imposed upon the employer for the defendant's illegal act of Internet gambling.[270]

76. In summary, an employer may be held liable for its employee's act of Internet gambling if: (1) the individual act of Internet gambling is illegal;[271] (2) the act occurred within the employee's scope of employment, such as providing Internet access to its employees;[272] and (3) the employer knew or should have known that the employee was gambling via the Internet at the workplace.[273]

---

[266] *See* Macavinta, *supra* note 264. The Providian National Bank situation described in the text is not the only time an individual has accused major credit card companies and banks of flagrantly violating state and federal laws by collecting debts incurred as a result of illegal Internet gambling. *See* Rovella, *supra* note 212. As of this writing, there are similar complaints filed in the state of Alabama and Wisconsin. *See id*.

[267] *See generally supra* note 237 (explaining that Internet gambling is illegal in the State of California).

[268] *See generally supra* notes 54-62 (discussing employer liability rational based on the fact that the employer's job created the opportunity for the employee to commit the wrongful or illegal act).

[269] *See generally supra* notes 51-64 (discussing when courts will hold an employer liable for its employee's illegal foreseeable acts).

[270] *See generally supra* Section II(B) (discussing what acts fall within the scope of the employee's employment).

[271] *See generally supra* Section III(A)(4)(a)-(b) (discussing current and future state and federal law addressing Internet gambling).

[272] *See generally supra* Section II(B) (discussing what acts fall within the scope of the employee's employment).

[273] *See generally supra* notes 51-64 (discussing when courts will hold an employer liable for its employee's illegal foreseeable acts).

B. Employer Policy: Defense and Prevention

77. If an employer provides its employees with Internet and e-mail access, then a clear computer policy must be implemented prohibiting the use of the Internet and e-mail for non-business and illegal activity.[274] The computer policy should be in writing and, if possible, it should be available in the employer's internal computer network.[275] Additionally, a signed copy of the computer policy should be collected from each employee having Internet or e-mail access.[276] It is also a good idea for employers to have their computer policy appear on the employee's computer screen immediately after their employees turn on their computer.[277]

78. The computer policy should also clearly define acceptable and unacceptable Internet and e-mail use.[278] The computer policy should warn all employees that any illegal conduct is strictly prohibited and will be grounds for disciplinary action including termination of their employment.[279] Moreover, employers should state in their computer policy that they are openly "monitoring" their employee's Internet and e-mail activities.[280] However, unless the employer requires each employee to read, comprehend and sign the policy, the adoption of this policy will not shield employers

---

[274] *See* Fernandez, *supra* note 6, at 840 (suggesting appropriate corporate policies regarding Internet use at the workplace); Peter Brown, *Policies for Corporate Internet and E-Mail Use*, *in* THIRD ANNUAL INTERNET LAW INSTITUTE, at 637, 670 (PLI Pat., Copyrights, Trademarks, & Literary Prop. Course Handbook Series No. G0-0051, 1999), *available in* WESTLAW, PLI/Pat File. For examples of computer policies, see University of California, *Electronic Mail Policy* (visited Feb. 7, 2000) <http://www.infowar.com/class_1/99/class1_072099a_j.shtml>; Archdiocese of Baltimore, *Computer Use & Internet Policy* (last modified Apr. 4, 2000) <http://www.archbalt.org/technology/policy.html>.

[275] *See* Brown, *supra* note 274, at 670.

[276] *See id.*

[277] *See* K. Robert Bertram, *Avoiding Pitfalls in Effective Use of Electronic Mail*, PA. B. ASS'N Q., Jan. 1998, at 11, *available in* WESTLAW, PABAQ File.

[278] *See* Brown, *supra* note 274, at 670, 672-73.

[279] *See* Terex Corp. v. UAW Local 1004, No. Civ. A. 2:97CV243-D-B, 1998 WL 433948, at *7 (N.D. Miss. June 17, 1998); Brown, *supra* note 274, at 670-71 (noting that the employer should inform its employees that transactions on the Internet, including e-mails, are not confidential and that such communication is being monitored).

[280] *See* Sally D. Garr, *Employee Monitoring and Privacy in the Internet Age*, *in* LEGAL PROBLEMS OF MUSEUM ADMINISTRATION 1, 5 (ALI-ABA Course of Study March 20, 1997), *available in* WESTLAW, ALI-ABA File. *See generally* Todd Wallack, *Firms Keep Online Users In Line*, BOSTON HERALD, Oct. 8, 1998, at 47, 47, 50 (explaining that employers monitor employees secretly and that privacy advocates object to the practice).

from liability.[281] Therefore, for the policy to shield an employer from liability effectively, the policy must be strictly enforced.[282]

79. In *Daniels v. Worldcom Corp.* the court held that the employer, Worldcom, avoided liability for its employee's wrongful act because the employer took prompt disciplinary actions as defined in its employee manual.[283] The employer, verbally and in writing, indicated to employees "the proper use of the [company's] e-mail system."[284] After the employer had knowledge of its employee's wrongful act of e-mail sexual harassment, it held two meetings to discuss its disciplinary policy against non-business activity on the company's e-mail system.[285]

80. Unfortunately, an employer's policy prohibiting non-business Internet activity can be a double-edged sword.[286] If the employer fails to enforce the policy or, upon "knowledge"[287] of its employee's wrongful act, fails to take prompt disciplinary action, then the employer's policy will not shield the employer from liability.[288]

81. Additionally, many large employers contend that monitoring all of their employee's Internet activity is impossible.[289] However, even if the "impossibility" was

---

[281] *See* Fernandez, *supra* note 6, at 840. If employers update all, or even one section of their employee computer use policy, then the employer must receive new consideration from each of their employees in order to shield themselves from liability. *See, e.g.*, Doyle v. Holy Cross Hosp., 708 N.E.2d 1140, 1145 (Ill. 1999) (holding that the employer's modification of the terms of its employee handbook or personnel policy would not be enforceable without new consideration).

[282] *See* Fernandez, *supra* note 6, at 840-41 (noting that statements indicating employee privacy may create liability if the employer accesses employee e-mail messages).

[283] No. CIV.A.3:97-CV-0721-P, 1998 WL 91261, at *5 (N.D. Tex. Feb. 23, 1998).

[284] *Id.* ("[A]n employer is not liable for the discriminatory actions of an employee when the employer . . . takes prompt remedial action . . . .").

[285] *See id.*

[286] *See NLRB Attacks Business-Only E-Mail Policy*, IOWA EMPLOYMENT L. LETTER, Nov. 1999, at 3 (noting that an NLRB opinion indicates that non-business use policy is an unfair labor practice if it is enforced selectively against employees making union-related communications); *see also* Terex Corp. v. UAW Local 1004, No. CIV.A. 2:97-CV-243-D-B, 1998 WL 433948, at *7 (N.D. Miss. June 17, 1998) (noting that once an employer has knowledge of its employee's wrongful act, the employer must act promptly with remedial action or face liability).

[287] An employer has knowledge of its employee's wrongful act when "they knew or 'should have known'" of the employee's wrongful act. Dermot Sullivan, Note, *Employee Violence, Negligent Hiring, and Criminal Records Checks: New York's Need to Re-Evaluate its Priorities to Promote Public Safety*, 72 ST. JOHN'S L. REV. 581, 593 (1998); *see* United States v. Ridglea State Bank, 357 F.2d 495, 498 (5th Cir. 1966) (holding that an employer can be held liable in criminal matters when an agent, without the actual knowledge of the employer, commits a specific intent crime).

[288] *See Daniels*, 1998 WL 91261 at *5.

[289] *See* Fernandez, *supra* note 6, at 837 (noting that software has been developed to assist in

proven by the employer, courts may still hold employers liable because of the modern trend of employer liability.[290]

82. Ironically, modern technology has some solutions. Software programs are available that will inform the employer when its employees are accessing prohibited websites.[291] These programs act like filters that identify unwanted words, phrases, or non-work related Internet sites and deny the employee access to the site.[292] This will allow the employer to take prompt disciplinary action in an effort to avoid liability.[293] Moreover, these programs are relatively inexpensive when compared to litigation.[294] Furthermore, a software program may reduce the risks of liability for an employee's copyright infringement of counterfeit or copied software.[295] However, courts may hold the employer's conduct of monitoring an employee to be an invasion of privacy,[296] unless

---

monitoring employee Internet activity but, because of the exponential growth of the Internet, and the impossibility of updating monitoring software to reflect new web sites, "employers should not expect to rely heavily on restricted access software in the future.").

290 The doctrine of respondeat superior holds that the employer will be strictly liable for the torts of its employee. *See* KEETON ET AL., *supra* note 54, § 69, at 499-500.

291 *See* Garr, *supra* note 280, at 5 (noting that "communications . . . may be monitored."). There are software companies, e.g., Elron Software Inc. and EG&G, Inc., "that can monitor every click of the mouse by employees, and can even block employees from accessing sites the company deems inappropriate." Joann Muller, *Troubles on the Internet: From Cyberloafing to Legal Questions About E-Mail Privacy, Worries Multiply as U.S. Firms Increasingly Go on Line*, BOSTON GLOBE, Oct. 23, 1998, at C1.

292 *See* Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS 629, 652-54 (1998). Lessig summarized some available software programs that the employer could utilize in blocking non-work related Internet sites in a thorough table. *See id.* at 653-54, n.66. Moreover, some companies are taking a pro-active stance and developed their own software to monitor all of its employees. *See* Wallack, *supra* note 280 (explaining how "Raytheon Corp. . . . developed it own software to keep tabs on 35,000 workers with Internet access;" and "[b]oth Bank Boston Corp. and Stride Rite Corp. . . . check employee's usage logs.").

293 *See Daniels*, 1998 WL 91261 at *5.

294 *See* Lessig, *supra* note 292, at 654 ("The software itself costs around $50; updates can cost between $10-$20 a cycle.").

295 *See* Mathiason & Barrett, supra note 132. According to a Computer World survey, "[a]bout 31% of 75 corporate e-mail managers already use monitoring software either regularly or for spot checks." Dominique Deckmyn, More Managers Monitor E-Mail, COMP. WORLD (visited Feb. 21, 2000) <http://www.computerworld.com/home/print.nsf/idgnet/991018C7D2>. Meanwhile, "State and Federal requests for wiretaps and bugs increased 12 percent in 1998 . . . ." Wiretapping, ELEC. PRIVACY INFO. CTR. (last modified Jan. 21, 2000) <http://www.epic.org/privacy/wiretap/>.

296 *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977). The Restatement provides that, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of privacy, if the intrusion would be highly offensive to a reasonable person." *Id.*

the employer has a formal policy on electronic communications in place about which it has informed its employees that all supervisors can read their e-mail.[297]

83. In addition to having a strictly enforced computer policy and using software to monitor employees' activity, employers may contract with monitoring service companies to search chat rooms and detect defamatory comments about the employer.[298] By utilizing these services, employers may be able to respond to defamatory comments.[299]

84. Furthermore, employers should install encryption software to protect confidential information.[300] This technology, however, is classified as a "munition" and may be subject to international laws "in dealings with other countries."[301] As a result, employers dealing with businesses outside of the United States should contact an attorney in order to ensure compliance with encryption laws.[302] Finally, employers should hire computer security consultants in order to prevent network security breaches.[303]

---

297 *See* Gibson v. Hummel, 688 S.W.2d 4, 7 (Mo. Ct. App. 1985) (explaining that an employer's secret surveillance of an employee is not prohibited by law unless it is outrageously intrusive); Hall v. May Dep't Stores Co., 637 P.2d 126, 129 (Or. 1981) (noting that adjectives such as 'outrageous' or 'intrusive' are "designed only to express the outer end of some gradation or scale of impropriety and social disapproval."); Trout v. Umatilla County Sch. Dist., 712 P.2d 814, 818 (Or. Ct. App. 1985) (discussing 'outrageous conduct'); *see also* Watkins v. L. M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (holding that an employer may monitor the employee's telephone call only long enough to determine whether it was business or personal in nature, where the employee had consented to monitoring of business calls only). For a detailed understanding of workplace monitoring, see generally Connie Barba, *"That's No 'Beep', That's My Boss:" Congress Seeks to Disconnect the Secrecy of Telephone Monitoring in the Workplace*, 21 J. MARSHALL L. REV. 881, 883-95 (1988); Steven Winters, Comment, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197, *passim* (1993).

Additionally, the Electronic Privacy Information Center in Washington, D.C. "is pushing for legislation that would force employees to let workers know if they're being watched." Wallack, *supra* note 280, at 50. At the state level, California tried to set workplace standards in monitoring employee's e-mail. *See* S.B. 1016, Reg. Sess. (Cal. 1999) *available in* WESTLAW, CA-BILLTXT File. However, on October 10, 1999, California Governor Gray Davis vetoed the bill. *See* S.B. 1016, Reg. Sess. (Cal. 1999) *available in* WESTLAW, CA-BILLTRK File.

298 *See* Mathiason, *supra* note 90.

299 *See id.* ("[T]he company can then post a corrective message and take any necessary legal action . . . .").

300 *See id.* ("This technology scrambles the information on the computer and makes it unreadable to everyone except the person with the encryption key.").

301 *Id.*

302 *See id.*

303 *See id.*

IV. CONCLUSION

85. Because access to the Internet makes it extremely easy to conduct illegal online activity, all employers are exposed to potential liability.[304] Although employees are rarely arrested for their illegal online activity,[305] employers must still protect themselves from potential liability. Not only should the employer be concerned about an employee's lost productivity when the employee is using the Internet for unauthorized activity, but it must also be concerned about being held liable for that employee's illegal online act.[306] An employer may never know if the government is monitoring its business activities, and if it is, employers beware, because the government has the capability to know what its employees are doing at their workplace.[307] To reduce the potential of employer liability, a strict company policy would act as a deterrent.

86. Employers who provide employees Internet access provide employees with the opportunity to conduct illegal online activity.[308] By allowing their employees the opportunity to conduct illegal activity, courts will consider the employee's illegal act

---

304 *See* Diana Kunde, *Privacy Clashes with Employer Need to Monitor E-Mail*, DALLAS MORNING NEWS (July 22, 1998), *available in* 1998 WL 13089225 (explaining that "e-mail is so effortless that employees 'are lulled into a false sense of security that may encourage overly blunt, abrupt, explicit, careless and otherwise ill-conceived messages'" and, along with "'the easy access to Internet porn and other potentially downloaded material, . . . you have a recipe for disaster . . . .").

305 *See, e.g.*, Robbins, *supra* note 204, ¶ 27 (noting that Professor I. Nelson Rose "'d[oes] not know of any case where a casual gambler has been arrested'" under California law).

306 *See generally* Klein, *supra* note 143, at 744 (noting that an employee's visit to pornographic Websites could subject an employer to liability for creation of a hostile work environment).

307 *See* Mark Boal, *Spycam City*, VILLAGE VOICE, Oct. 6, 1998, at 38, *available in* 1998 WL 20492919 (noting that "the F.B.I. clamors for the means to monitor any cell-phone call. Meanwhile other government agencies are developing schemes of their own."). Information on the various federal and state agencies and private entities patrolling the Internet is provided in *Here Come the Cybercops 3: Betting on the Net*, a paper presented at the Twenty-Sixth Popular Culture Association and Twentieth American Culture Association Annual Conf. in Orlando, Florida on Apr. 8-11, 1998. *See* Koegler, *supra* note 234, at 545 n.*. The federal government prosecuted fourteen owners or managers of six Caribbean or Central America Internet gambling sites for "conspiring to illegally transmit bets over the Internet and telephone." Mike Bruker, *First Web Bettors Prosecuted*, MSNBC (visited Nov. 19. 1999) <http://www.zdnet.com/zdnn/content/msnb/0305/291901.html>. When Attorney General Janet Reno made the announcement of the criminal complaint, she warned everyone that the federal government will enforce federal law addressing illegal online activity. *See id.*; *see also* Bill Pietrucha, *Feds Bag Online Bookies*, NEWSBYTES, Mar. 5, 1998, *available in* 1998 WL 5031916.

308 *See generally supra* notes 54-62 (discussing employer liability rationale based on the fact that the employer's job created the opportunity for the employee to commit the wrongful or illegal act).

within the scope of employment and may hold the employer liable for the employee's illegal online activity.[309] Furthermore, if the employer is located in a state were the individual act of Internet gambling is illegal, the employer may be held liable for its employee's illegal act of Internet gambling.[310] To minimize the risk of employer liability for illegal online activities of its employees, employers must establish a strict company policy prohibiting employees' illegal online act.[311] Moreover, a strictly enforced company policy puts employees on notice that the employer is monitoring their activity.[312] As technology advances, the employer must keep pace with this growth to avoid legal chaos.[313]

---

[309] *See generally supra* Section II(B) (discussing acts within the scope of the employee's employment).

[310] *See generally supra* notes 235-57 and accompanying text (discussing current state law that prohibits Internet gambling).

[311] *See generally supra* Section III(B) (discussing employer policy as a defense).

[312] *See generally supra* Section III(B).

[313] For a list of state statutes relating to computer related crimes, see *supra* note 165. For articles discussing various developments in computer law, see generally Eric Schwartz & Michael Schlesinger, *Washington Watch*, CYBERSPACE LAW., June 1997, at 16, *available in* WESTLAW, GLCYLAW File; Jon Baumgarten & Denise Gough, *Washington Watch*, CYBERSPACE LAW., Sept. 1998, at 16, *available in* WESTLAW, GLCYLAW File; Jon A. Baumgarten et al., *Washington Watch*, CYBERSPACE LAW, May 1998, at 20, *available in* WESTLAW, GLCYLAW File; and Jon A. Baumgarten et al., *Washington Watch*, CYBERSPACE LAW, Apr. 1998, at 30, *available in* WESTLAW, GLCYLAW File.