REDUCING THE LIABILITY RISKS OF EMPLOYEE MISUSE OF THE INTERNET

BLAKE A. BELL
SIMPSON THACHER & BARTLETT LLP

JUNE 30, 1999

A company suspects that its own employees are anonymously posting confidential company data to an Internet message board and is forced to file suit to learn their identities. The Dean of the Divinity School of an ivy-league university is forced to resign after sexually-explicit images are discovered on his university-owned computer. A brokerage firm dismisses 19 employees after they fail to admit that they have used the firm's e-mail system to distribute racist jokes and sexually explicit material. Someone posts a fake Web page announcing that a technology company is an acquisition target and drives the company's stock price up 31% before the hoax is revealed. The perpetrator is arrested and identified as one of the company's own employees. An employee with the deadly AIDS virus uses a company computer to access a chat room and to lure a young woman to have sex. She contracts the deadly disease and sues the company to hold it liable for its employee's misconduct while he was on the job.

While these might seem like the bad dreams of an overworked investor relations professional, all are incidents that actually have occurred.[1] As Internet access becomes ubiquitous in the American workplace, so has employee misuse of the Internet. What many employers may not recognize, however, is that they may bear liability risks for the online misconduct of their employees.

How can companies with employee Internet access reduce their liability risks? There are steps to take. The first, of course, is to understand the risks.

The many forms of online employee misconduct seem limited only by the fertile imaginations of an increasingly Internet-savvy workforce. Any effort to categorize all such misuses or to suggest that an exhaustive list is even possible is doomed from the outset. Yet, there are at least several categories of potential employer liability risks that merit special consideration. They include violations of the securities laws, harassment and discrimination, cyberlibel and online copyright infringement.[2]

Securities Law Violations

On April 7, 1999, three minutes before the nation's financial markets opened, a posting appeared on a Yahoo! Finance message board. The posting said "BUYOUT NEWS!!! ECILF is buying [PAIRGAIN TECHNOLOGIES] . . . Just found it on Bloomberg". The posting included a hyperlink to a Web page that appeared to be part of Bloomberg L.P.'s news site. That page, in turn, 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." PairGain's stock price quickly raced from $8-1/2 to $11-1/8 — nearly a 31% increase — before the markets settled and the share price fell back.[3]

The following week, an army of cybersleuths identified the perpetrator of the posting as Gary D. Hoke Jr., a 25-year-old PairGain employee located in Raleigh, North Carolina. On April 12, Bloomberg L.P. filed a lawsuit seeking unspecified damages and injunctive relief against "John Does 1 through 5" in the United States District Court for the Southern District of New York.[4] On April 14, the U.S. Attorney's Office in Los Angeles filed a complaint in federal court against Hoke alleging securities fraud punishable by up to ten years in prison and a $1 million fine.[5] On April 15, Mr. Hoke was arrested at his home.[6] On April 21, the U.S. Securities and Exchange Commission filed a complaint against Hoke in the United States District Court for the Central District of California alleging that Hoke's scheme constituted manipulation of the price of PairGain's publicly-traded securities in violation of the Securities Exchange Act of 1934 and Rule 10b-5 promulgated under that Act.[7]

Through all this, PairGain cooperated fully in the investigation. There never was any allegation that anyone else at PairGain was involved in the scheme. Yet, 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.

Such doubts would have been well founded. If an employee of a company whose stock is publicly traded uses a message board, chat room or e-mail to commit securities fraud, through a stock manipulation scheme[8] or otherwise, there is at least a risk in some jurisdictions that the company could be sued under a theory of "respondeat superior" to answer for its employee's misconduct. Granted, there is a raging debate over whether respondeat superior liability survived the decision in *Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164 (1994), but the fact remains that in some jurisdictions, courts have held that such a theory remains viable.[9]

Additionally, participation by employees of public companies in electronic debates, discussions and arguments via the Internet can lead to unwitting disclosures that are materially inaccurate and, thus, violate the general antifraud provisions contained in Rule 10b-5. As one recent analysis puts it, quite succinctly:

Employees have also been known to enter into discussions regarding their employers in these online forums. Perhaps participants are degrading the company and an employee responds with a defense, noting his corporate affiliation in an effort to add credibility to the defense. In such a setting, it is unlikely that the employee would use the caution exercised by company executives in issuing public statements. Although the employee may not be authorized to speak on the company's behalf, the participants might reasonably perceive otherwise. Such statements could be treated as disclosures by the company. The problem is exacerbated by the fact that persons participating in chat rooms and similar forums tend not to take their communications as seriously as the law warrants. They do not realize the potential pitfalls.[10]

Harassment and Discrimination

Employees have relied on e-mail messages as the basis of suits for racial and sexual harassment against their employers. In 1995, Chevron Corporation reportedly paid a settlement in excess of $2.2 million after four female employees sued the company following receipt of e-mails that allegedly were sexually harassing.[11] Similarly, black employees sued Morgan Stanley & Co. In 1996 alleging racial discrimination based on e-mails distributed by other employees. The case reportedly was settled in February 1998.[12] There have been numerous other such suits as well.[13]

Cyberlibel

In recent years, companies have had to cope with false Internet rumors posted to electronic message boards and published in chat rooms. Increasingly, companies have chosen to file defamation suits against those who post such rumors.[14] One company, however, recently found itself involved in a strange new twist on that old story.

Last February, Massachusetts-based Raytheon Company discovered a Yahoo! Finance message board containing messages critical of the company and its operations. While many other companies have experienced the same scenario, Raytheon observed that some of the messages contained information that it believed was not public knowledge and could only have been posted by company employees. The company filed suit in Middlesex County, Massachusetts against 21 "John Does" and promptly served a subpoena on Yahoo! Inc. seeking information regarding the identities of those who made the anonymous postings.[15] Ultimately, a group of employees who had posted anonymous messages to the board was identified.

Four Raytheon employees subsequently resigned and the rest "entered corporate 'counseling.'" Raytheon then dismissed its lawsuit, claiming that its "internal investigation had accomplished what we wanted it to accomplish."[16]

Other cyberlibel suits arising from employees' use of the Internet have been filed as well. For example, a company's former employee prevailed in a cyberlibel suit against the company after a company employee sent an e-mail to a third party stating that the former employee was

terminated for "credit card abuse."[17] In addition, a British lecturer recently sued a graduate student / teaching assistant as well as his University employer for cyberlibel after the student used his employer's computer network to post allegedly defamatory statements to a Usenet news group.[18]

The ease with which e-mail messages may reach a global audience, as well as the propensity for employees to treat such communications as little more than a quickly-created personal note can be a recipe for disaster. As one group of commentators has noted:

> General guidelines already exist relating to the issue of employees who defame others under the auspices of the company. However, with the Internet, the opportunity for harm is greater, as employees can more easily disseminate information to a wide range of media. Employees participating in chat rooms, newsgroups or even sending E-mail under their employers' domain names can place the company at risk for being sued . . .[19]

Online Copyright Infringement

In certain circumstances, an employer can be held liable for copyright infringement committed by an employee. Indeed, in one widely-watched case, a trade organization was found liable for copyright infringement after its employee who was responsible for its Web site used copyrighted clip art on the Web site. According to the court, the trade organization could not rely on an "innocent infringer" defense "because the defense may be raised only when the infringer relied on an authorized copy that omitted the copyrighted notice. In this case, [the employee] relied on unauthorized copies of plaintiff's clip art files."[20]

As with defamation claims, the risk of online copyright claims as a result of employee misconduct is a very real one. The very nature of the Internet and, more particularly, the Web, make it easy to copy and to forward or publish copyrighted images or content. Moreover, as the National Association of Fire Equipment Distributors discovered, liability can result from what may otherwise seem the to be the most innocent of activities.[21]

What Can A Company Do To Reduce Its Risks?

There are many steps a company can take to reduce its risk of liability from employee misuse of the Internet. What follows are a few of the most important considerations to keep in mind.

Create and distribute to all current and new employees a carefully-crafted Internet use policy. Examples of such policies are widely available.[22] At a minimum, the policy should:

- Address to what extent personal use of the firm's systems will be permitted;
- Emphasize that the firm's systems are its property and are intended for legitimate business use;

- Prohibit use of the firm's systems for unlawful, unethical, defamatory, tortious or offensive activities;

- Prohibit use of the systems to access or to disseminate obscene, pornographic or sexually explicit material;

- Prohibit use of the firm's systems to infringe or otherwise to misuse either the firm's or third parties' trade secrets, confidential business information, copyrighted materials or other intellectual property;

- Require that employees take steps to protect their personal passwords and refrain from accessing or reading others' e-mails or computer data when not otherwise authorized to do so;

- Inform employees that the firm reserves the right to monitor e-mails and employees' use of the Internet; and

- Inform employees of the procedures that will be followed and the consequences that may result if the Internet use policy is not followed.[23]

Wherever possible, obtain adequate insurance. Confirm that claims for defamation, patent, copyright and trademark infringement and other such claims are covered.[24]

Consider electronic monitoring of employee e-mail and Internet activity. Remember, however, that monitoring programs must be implemented consistently with a host of applicable statutory, regulatory and common law requirements intended to protect employees' privacy interests and constitutional rights. Such programs should not be implemented in the absence of coordination with counsel experienced in applicable privacy issues, labor law, state statutes limiting employee monitoring programs and constitutional issues that may apply particularly when public employers are involved.[25]

Consider the use of filtering devices to block access to inappropriate Web sites, chat rooms, message boards and Usenet news groups. Once again, however, such a program must be implemented with care and with participation by counsel.[26]

Perhaps the single most important thing that can be done is simply to make employees aware of the consequences that may arise from their misuse of the Internet — including the risk to the company as well as the risk of their own personal liability.

Blake A. Bell is Senior Knowledge Management Counsel at Simpson Thacher & Bartlett LLP in New York City. He focuses on computer-related matters, Internet Law, securities regulation and commercial litigation. He can be reached at B_Bell@stblaw.com. The views expressed herein are not necessarily those of his firm.

ENDNOTES

1 *See, e.g.,* Todd Wallack, *Staffers Stunned by Net Lawsuit*, BOSTON HERALD, Mar. 5, 1999, 1999 WL 3391860 (Raytheon Co. files suit against John Does who turn out to be company employees who allegedly leaked confidential company data via an Internet message board); Fox Butterfield, *Pornography Cited in Ouster of Harvard Divinity School Dean*, N.Y. TIMES ON THE WEB, May 20, 1999 (available via search at http://www.nytimes.com); *Arrest Made in PairGain Stock Scam*, ASSOCIATED PRESS SPECIAL TO ZDNN TECH NEWS NOW, Apr. 15, 1999 <http://www.zdnet.com/zdnn/stories/news/0,4586,2242474,00.html>; Geanne Rosenberg, *Heard it on the PC Grapevine*, N.Y. TIMES ON THE WEB, May 23, 1999 (available via search at http://www.nytimes.com)(noting brokerage firm Edward D. Jones recently fired 19 people who it said failed to admit that they had sent pornography or off-color jokes via e-mail); *Haybeck v. Prodigy Servs. Co.*, 944 F. Supp. 326 (S.D.N.Y. 1996).

2 *See generally* Stuart Rosove, *Employee Internet Use: Big Brother Gets Involved - Employer Liability Remains Unclear*, N.Y.L.J., Mar. 17, 1997 <http://ljx.com/practice/laboremployment/0317empl.html>; Jeffrey S. Nowak, *Note: Employer Liability for Employee Online Criminal Acts*, 51(2) FED. COMM. L.J. 467 (Mar. 1999) <http://www.law.indiana.edu/fclj/pubs/v51/no2/nowakmac.PDF>.

3 *See* Matthew Broersma and Larry Barrett, *Bogus Report Boosts Internet Stock*, ZDNN TECH NEWS NOW - BUSINESS, Apr. 7, 1999 <http://www.zdnet.com/zdnn/stories/news/0,4586,2238191,00.html>; *see also* Edward Wyatt, *Fake Internet News Account Sends a Stock Price Soaring*, N.Y. TIMES ON THE WEB, Apr. 8, 1999 (available via search at http://www.nytimes.com/); Jonathan Gaw, *Internet Hoax Sends O.C. Tech Stock Up 31% - Cyberspace: False Detailed Report that PairGain Was Being Acquired Illustrates Growing Potential for Net Fraud*, L.A. TIMES, Apr. 8, 1999, at A-1.

4 *Bloomberg Files Lawsuit Over False Story*, ASSOCIATED PRESS SPECIAL TO N.Y. TIMES ON THE WEB, Apr. 13, 1999 (available via search at http://www.nytimes.com/).

5 *See FBI Arrests Man Charged With Posting Fake News Report*, ASSOCIATED PRESS SPECIAL TO N.Y. TIMES ON THE WEB, Apr. 15, 1999 (available via search at http://www.nytimes.com/).

6 *See FBI Arrests Man Charged With Posting Fake News Report*, ASSOCIATED PRESS SPECIAL TO N.Y. TIMES ON THE WEB, Apr. 15, 1999 (available via search at http://www.nytimes.com/).

7 *See Securities and Exchange Commission v. Gary D. Hoke, Jr.,* Civ. Action No. 99-04262 (LGB) (Ex) (complaint filed Apr. 21, 1999); *see also* SEC Litig. Rel. No. 16117 (Apr. 21,

1999) <http://www.sec.gov/enforce/litigrel/lr16117.txt>; *SEC News Digest: Enforcement Proceedings*, No. 99-77, Apr. 22, 1999 <http://www.sec.gov/news/digests/04-22.txt>.

8 There are a number of provisions of the Exchange Act of 1934 that arguably prohibit the manipulation of stock prices through false or misleading Internet communications including: (i) Section 10(b), 15 U.S.C.A. § 78j(b); (ii) Rule 10b-5, 17 C.F.R. § 240.10b-5 (1996); (iii) Rule 10b-1, 17 C.F.R. § 240.10b-1; (iv) Section 9(a)(2), 15 U.S.C.A. § (v) Section 9(a)(3), § 78i(a)(3); and (vi) Section 9(a)(4), 15 U.S.C.A. § 78i(a)(4).

9 *See, e.g., Seolas v. Bilzerian,* 1997 U.S. Dist. LEXIS 1036 (D. Utah, Jan. 28, 1997); *Pollack v. Laidlaw Holdings, Inc.,* [1995 Binder] Fed. Sec. L. Rep. (CCH) ¶ 98,741, at 92,497 (S.D.N.Y., May 2, 1995). *See also* Robert A. Prentice, *The Future of Corporate Disclosure: The Internet, Securities Fraud, and Rule 10B-5,* 47 EMORY L.J. 1, 77 n.345 (Winter 1998).

10 *See* Daniel L. DeWolfe, Eric M. Roth & Douglas Bernstein, *Legal Watch: The Liability of Public Companies for Reports in Internet Chat Rooms*, AlleyCat News, Mar. 1999, at 22, 22-23 (AlleyCat Information Sciences, Inc.).

11 Susan E. Gindin, *BNA Corporate Practice Series: Guide to E-Mail and the Internet in the Workplace* at 12 (BNA 1999) (citing Michelle Singletary, *Loose Lips an E-Mail Hazard*, WASH. POST, Apr. 6, 1997, at F12).

12 Gindon, *Guide to E-Mail and the Internet in the Workplace* at 12; *Owens v. Morgan Stanley & Co.,* No. 96 Civ. 9747, 1997 WL 403454 (S.D.N.Y. July 17, 1997).

13 *See, generally,* Gindin, *Guide to E-Mail and the Internet in the Workplace* at 34-36 & 34 n.110; Louise Ann Fernandez, *Workplace Claims: Guiding Employers and Employees Safely in and out of the Revolving Door* (1997) <http://www.pli.edu/arts/Workplace_Claims.htm>; *see also Owens v. Morgan Stanley & Co.,* No. 96 Civ. 8747, 1997 WL 793004 (S.D.N.Y. Dec. 24, 1997) (permitting suit alleging discrimination and retaliation after they complained about e-mail to proceed); *Jones v. RR Donnelley & Sons, Inc.,* No. 96C 0007717 (N.D. Ill., complaint filed Nov. 26, 1997) (employees sued company for harassment and racial discrimination after racial, ethnic and sexual jokes allegedly were distributed via the company's e-mail system); *Curtis v. Citibank, N.A.,* No. 97-1064 (S.D.N.Y. 1997) (employees filed purported class action alleging that racial jokes and offensive materials were distributed via the company's e-mail system); *Daniels v. WorldCom Corp.,* 1998 WL 91261 (N.D. Tex. 1998) (court rejected employees' suit alleging harassment and other misconduct in violation of Title VII of the Civil Rights Act of 1964 and 42 U.S.C. §§ 1981 & 1983 arising from e-mail jokes distributed by another employee).

14 *See* Blake A. Bell, *Dealing With False Internet Rumors: A Corporate Primer,* 2(7) WALLSTREETLAWYER.COM 1 (Glasser LegalWorks Dec. 1998).

15 *See* Todd Wallack & Andrea Estes, *On the Internet, You're Not So Anonymous, After All*, BOSTON HERALD, Mar. 5, 1999, 1999 WL 3391767; Todd Wallack, *Staffers Stunned by Net Lawsuit*, BOSTON HERALD, Mar. 5, 1999, 1999 WL 3391860.

16 Tom Kirchofer, *Raytheon Drops Internet Chat Suit*, YAHOO! NEWS, May 21, 1999 (available via search at http://dailynews.yahoo.com); *Raytheon Drops Suit Over Internet Chat*, ASSOCIATED PRESS SPECIAL TO N.Y. TIMES ON THE WEB, May 22, 1999 <http://www.nytimes.com/library/tech/99/05/biztech/articles/22raytheon.html>; William M. Bulkeley, *Tech Crime: Raytheon Employees Resign in Wake of Lawsuit Protesting Internet Postings*, WALL ST. J. INTERACTIVE ED., Apr. 5, 1999 (available via search at http://interactive.wsj.com); Todd Wallack, *Business Today: Message Nets VP an Exit*, BOSTON HERALD.COM, Mar. 31, 1999 <http://www.businesstoday.com/topstories/ray03311999.htm>.

17 *See Meloff v. New York Life Ins. Co.*, 51 F.3d 372 (2d Cir. 1995).

18 *See Laurence Godfrey v. Cornell University,* High Court of Justice (U.K.) (complaint filed Oct. 1997).

19 Stuart Rosove, *Employee Internet Use: Big Brother Gets Involved - Employer Liability Remains Unclear,* N.Y.L.J., Mar. 17, 1997 <http://ljx.com/practice/laboremployment/0317empl.html>; *see also* Gindon, *Guide to E-Mail and the Internet in the Workplace* at 12-13.

20 *See Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equipment Distributors*, 983 F. Supp. 1167, 1174 (N.D. Ill. 1997) <http://www.bna.com/e-law/cases/marobie.html>.

21 A host of other employee activities can place employers at risk of liability including computer hacking while on the job, downloading pornography from the Internet, distribution of electronic threats and other such misdeeds. *See* Rosove, *Employee Internet Use*, N.Y.L.J., Mar. 17, 1997 <http://ljx.com/practice/laboremployment/0317empl.html>.

22 *See, e.g.,* Gindon, *Guide to E-Mail and the Internet in the Workplace* App. A at 61-62 and App. B at 65-67.

23 For a more detailed description of issues that should be addressed in an all-encompassing Internet use policy, *see* Jeffrey S. Nowak, *Note: Employer Liability for Employee Online Criminal Acts*, 51(2) FED. COMM. L.J. 467, 486-88 (Mar. 1999) <http://www.law.indiana.edu/fclj/pubs/v51/no2/nowakmac.PDF>.

24 *See* George B. Delta & Jeffrey H. Matsuura, *Law of the Internet*, Appendix 13 at App. 13-1 (Aspen Law & Bus. 1998).

25 *See, generally* Gindon, *Guide to E-Mail and the Internet in the Workplace* at 37-42.

26 For example, although the decision ultimately was reversed, state restrictions on the ability of state employees to access sexually-explicit Web sites were held by one court to be an unconstitutional violation of the First Amendment to the U.S. Constitution in *Urofsky v. Allen*, 995 F. Supp. 634 (E.D. Va. 1998) <http://www.Loundy.com/CASES/Urofsky_v_Allen.html>, *rev'd*, 167 F.3d 191 (4th Cir. 1999).