BENDER'S CALIFORNIA
LABOR & EMPLOYMENT
BULLETIN

Vol. 2005, No. 10 • October 2005

Michael C. Sullivan, Editor-in-Chief

Inside This Issue

What Employers Should Know (and Do) About Blogs

By Shawna M. Swanson and Patrick Sherman

Introduction and Overview

Why Should Employers Care About Weblogs?
With the proliferation of weblogs or "blogs," companies find themselves faced with a new forum for employee conduct that poses both risks and rewards. News reports of employees being terminated because of the content of their blogs abound, as do complaints by such employees that they did not have notice that their conduct was problematic. Yet, many companies are encouraging their employees to blog, even teaching them how to do so effectively.

Some companies have taken a hard line on blogging, terminating employees for the content of their blogs. In an apparent backlash to the way some companies have treated employees because of their blogs, The Blogger's Rights Blog has created an International Blogger's Bill of Rights along with a list of "blogophobic" companies, who "will be blacklisted by millions of bloggers the world over."[1] The site currently lists 49 entities, including Delta Airlines, Wells Fargo, and Harvard, all of which terminated employees, partly because of the employees' personal blog.

In contrast, other companies have chosen to express their support for blogging and have published blog guidelines. Many companies, especially those in the technology sector, actively use internal company blogs for collaboration. Some not only expressly

[1] *See The Blogger's Rights Blog, International Blogger's Bill of Rights*, available at http://rights.journalspace.com/?b=1104566400&e=1105171200 (last modified July 7, 2005).

(Continued on page 353)

A NOTE ON CITATION: The correct citation form for this publication is: 2005 Bender's Calif. Lab. & Empl. Bull. 351 (October 2005)

Editorial Note:

In the July/August issue of *Bender's CA Labor & Empl. Bull.* article entitled *California's "Reasonable Particularity" Requirement in Trade Secret Litigation* by Tyler M. Paetkau, the following author credits were inadvertently omitted:

California's "Reasonable Particularity" Requirement in Trade Secret Litigation by Tyler M. Paetkau and Princeton H. Kim, Winston & Strawn LLP. Mr. Paetkau is a partner in the San Francisco Office and Mr. Kim is an Associate in the Los Angeles Office of the Labor and Employment Relations Department of Winston & Strawn LLP. Messrs. Paetkau and Kim are grateful for the invaluable assistance of Kamala Haake, Cornell Law School, J.D. expected 2006, Winston & Strawn Summer Associate, in the preparation of this Article.

What Employers Should Know (and Do) About Blogs

By Shawn M. Swanson* and Patrick Sherman**

**Shawna M. Swanson is the partner leading Fenwick & West LLP's San Francisco-based Employment Practices Group. **Patrick Sherman is an associate in Fenwick & West LLP's Mountain View office.*

(Continued from Page 351)

encourage employees to create blogs, but provide the tools necessary to do so. Among the reasons cited for such a policy is the view that blogs can be an effective tool to communicate and gather information about the company, its products, its partners, and/or its customers. Other companies adopt policies based on a less-than-enthusiastic recognition that they cannot prohibit employees from blogging and therefore prefer to provide guidelines for employees about appropriate blog-related conduct and content.

What is a Blog?

A blog is a webpage through which a person catalogues and comments on other online resources. As described by Internet guru Dave Winer:

"Weblogs are often-updated sites that point to articles elsewhere on the web, often with comments, and to on-site articles. A weblog is a kind of continual tour, with a human guide who you get to know. There are many guides to choose from, each develops an audience, and there's also comraderie and politics between people who run weblogs, they point to each other, in all kinds of structures, graphs, loops, etc."[2]

A blogger maintains control over the content of the posting, but can let others comment on the information. In this way, a blog differs from a Wiki (or WikiWikiWeb), which "is a web application that allows users to add content, as on an Internet forum, but also allows *anyone* to edit the content."[3]

The term "blog," however, appears to have taken on greater significance. According to *Webopedia*, an online encyclopedia about computer technology, a blog "is a Webpage that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author."[4]

Blogs have become increasingly easy to create and maintain. Companies such as Google (http://www.blogger.com) and MSN (http://spaces.msn.com) have developed tools and provided server space for even the least computer-savvy person to post a blog.

Why the Recent Interest in Blogging?

According to the Internet World Stats website, which regularly tracks and posts population and Internet usage statistics, as of July 23, 2005,[5] over 938 million people worldwide use the Internet.[6] That figure represents a 160% growth from 2000 to 2005. Blogs, one component of the Internet, have more recently experienced increased popularity. According to *The Blog Herald*,[7] which regularly tracks and reports on the number of blogs based on information compiled through the Internet, there are over 70 million blogs on the Internet as of July 2005.[8]

As for blog use in the United States, comScore Networks recently released a report detailing the scale, composition, and audiences of blogs. The report, which was sponsored in part by Six Apart and Gawker Media, found that nearly 50 million Americans, or about 30 percent of the total U.S. Internet population, visited blogs in Q1 2005. This represents an increase of 45 percent compared to Q1 2004.[9]

Why the proliferation? Blogs provide a quick and easy (and sometimes anonymous) way to communicate a message to a potentially vast audience. For instance, bloggers, who may fancy themselves

---

[2] Dave Winer, *Weblogs.com: History of Weblogs*, available at http://newhome.weblogs.com/historyOfWeblogs (last updated May 17, 2002).

[3] *Wikipedia*, "*wiki*," available at http://en.wikipedia.org/wiki/Wiki (last visited July 12, 2005).

[4] *Webopedia*, "*blog*," available at http://www.webopedia.com/TERM/b/blog.html (last visited June 12, 2005).

[5] Internet World Stats, available at http://www.internetworldstats.com.

[6] Internet World Stats, *Internet Usage Statistics – The Big Picture, World Internet Users and Population Stats*, available at http://www.internetworldstats.com/stats.htm (last visited July 23, 2005).

[7] *The Blog Herald*, available at http://www.blogherald.com.

[8] *The Blog Herald, Blog Count for July: 70 million blogs* (July 2005), available at http://www.blogherald.com/2005/07/19/blog-count-for-july-70-million-blogs/.

[9] *Behaviors of the Blogosphere: Understanding the Scale, Composition and Activities of Weblog Audiences*, available at http://www.comscore.com/blogreport/comScoreBlogReport.pdf.

investigative reporters, have contributed to (and, in some instances, shaped) national discourse and impacted mainstream media reporting, including during the 2004 Presidential election. Bloggers have been recognized for (1) investigating and creating mainstream interest in the Swift Boat Veteran ads, and (2) discrediting the news source underlying CBS's *60 Minutes* story on President George W. Bush's National Guard service.[10] Politics is not the only purpose for blogging; some people may blog to communicate with friends and family and others may blog as a leisure activity.

The Risks of Encouraging Employees to Blog

Companies are constantly responding to a changing technological environment. From handwriting to typewriters, to word processors, to computers, each step has facilitated quicker and more widespread communication. Most recently, companies have dealt with new challenges surrounding electronic communications such as email and instant messaging (IM): specifically, protecting employer trade secret information, preventing harassment, and protecting employee privacy. Facing challenges related to blogs is simply the next step: the same law in a new context.

Legal Risks

Harassment

Courts likely will analyze a harassing blog just as they would any other communication (such as an email, a comment, or a picture) that contributes to an intimidating, offensive, or hostile work environment. That is, the courts will consider the following:

- Is it unwelcome?
- Is it based on sex or another protected category, such as age, race or religion?
- Is it sufficiently severe or pervasive to alter the recipient's conditions of employment?
- Does it create an intimidating, hostile or offensive work environment?
- Was the employer aware (or should the employer have been aware) of the conduct, and did it fail to prevent or remedy it?

In one of the first decisions involving sexual harassment in cyberspace, the New Jersey Supreme Court determined that an employer may be liable for its employees' electronic posts to a bulletin board. In *Blakey v. Continental Airlines*,[11] plaintiff Tammy Blakey sued Continental Airlines and several of its male pilots for, among other claims, defamation and sexual harassment based upon a hostile workplace environment. Blakey, the airline's first female captain to fly an Airbus aircraft seating 250 passengers, claimed the airline's pilots published defamatory and harassing electronic messages on a computer bulletin board called the Crew Members Forum. The Forum was accessible to all Continental pilots and crew members through an Internet provider, CompuServe. While Continental Airlines required that pilots and crew access CompuServe to learn their flight schedules and assignments, the Crew Members Forum was voluntarily accessed by crew members to exchange ideas and information, at their own cost. Blakely claimed that the pilots' offensive postings constituted sexual harassment and discrimination. These postings included "If the porn bothers you, don't look," and "Now don't start your feminazi routine with me."

The New Jersey Supreme Court ruled that sexual harassment and other forms of workplace discrimination can give rise to liability when they occur in cyberspace, as well as in a physical space that the company controls.[12] While holding there was no strict obligation on the part of the airline to monitor the bulletin board, the court ruled that the airline was obligated to redress complaints of harassment.[13] Recognizing that an electronic bulletin board may not have a physical location within a terminal or an aircraft, the court ruled that it nevertheless may be so closely related to a workplace environment, and so beneficial to the functioning of the airline, that the Forum should be regarded as part of the workplace in determining whether harassment occurred.[14] In addition, the court found that personal jurisdiction existed over the defendant pilots since Continental Airlines had its headquarters and main operations in New Jersey, and there were sufficient contacts within that state, notwithstanding that the alleged cyberspace harassment had no particular geographical, territorial presence.[15]

Parallels between the posting of a message to a bulletin board and creating and maintaining a blog, make *Blakey's* analysis of the sexual harassment claim

---

[10] The Write News, *Blogs Popular During 2004 Election* (November 5, 2004), available at http://www.writenews.com/2004/110504_blogs_intelliseek.htm; *see also Intelliseek's Blogpulse: Campaign 2004 Radar*, available at http://www.blogpulse.com/politics/politics_summary.html (survey of blog usage compared to other online media as well as subject of blogs accessed).

[11] 164 N.J. 38 (2000).

[12] *Id.* at 46.

[13] *Id.*

[14] *Id.*

[15] *Id.*

particularly relevant: both involve an electronic message available in cyberspace and voluntary access to the electronic communications. Under such circumstances, according to *Blakey*, the communication is relevant to (and can be the basis for) a hostile work environment claim.

The type of blog – personal or corporate – may also factor into the analysis. In *Blakey*, the court noted that where the electronic communication was closely related to the workplace and the employer benefited from the communication, it may be considered part of the workplace for purposes of determining whether the communication creates a hostile work environment.[16] Thus, a company-sponsored blog will likely be considered a part of the workplace in evaluating whether a posting to the blog creates a hostile work environment. In any event, as the *Blakely* court determined, an employer has an obligation to investigate all reports of sexual harassment – whether the harassment involves a personal or a corporate blog.

Discrimination

An employer's adverse action based on the content of a blog is governed (and limited) by the same anti-discrimination laws and standards applied to other adverse employment actions. An employer may not terminate or discipline the employee based on a protected characteristic. Stated another way, an employer must enforce its policies (including its blog policy, if it has one) without regard to any protected characteristic, including race, sex, age, national origin, disability, and sexual orientation.

A former Delta Airlines flight attendant has challenged her termination, purportedly for the content of her blog, as unlawful sex discrimination. Ellen Simonetti filed a claim with the Equal Employment Opportunity Commission against her former employer, Delta Airlines. Ms. Simonetti alleged that she was terminated for posting several images on her blog. Among the images was a photograph of Ms. Simonetti posing in her flight attendant uniform in a mildly suggestive pose. Ms. Simonetti claims her termination constituted sex discrimination because Delta Airlines had not disciplined or terminated male colleagues for similar conduct. To date, no decision has been reported on Ms. Simonetti's complaint.

Employers should take a cue from this complaint and act consistently from employee-to-employee when imposing discipline.

Privacy

Employers may have a number of reasons to monitor Internet usage or to identify the author of a blog. For instance, an employer may need to review the content of a blog and determine its author to investigate a complaint of harassment. Further, an employer may wish to monitor employee Internet usage (including access to and use of personal blogs) to determine whether employees are engaged in wrongdoing or to confirm that employees are spending their time on productive business rather than surfing the Internet or attending to personal matters. In fact, a 2005 survey released by the American Management Association and ePolicy Institute[17] indicates that, of the companies participating in the survey:

- 26% had terminated employees for Internet misuse;
- 75% monitor employee Website connections;
- 65% use software to block connections to inappropriate Internet content (which represents a 27% increase since the 2001 survey); and
- 86% monitor computer usage;
- 36% track content, keystrokes and time spent on the keyboard (with 80% of those employers notifying employees of their monitoring policy); and
- 50% store and review computer files (with 82% of those employers notifying employees of the monitoring policy).[18]

Such actions may expose a company to an allegation of invasion of privacy.

Although the case law is still sparse, courts have generally upheld employer interests in monitoring the use of their computer systems. While the case law recognizes an employer's right to *monitor* employee use of the company network, traditional labor and employment law (as discussed above) may restrict the employer's ability to *act upon* that information in formulating employment decisions.

Reasonable Expectation of Privacy

Regardless of the source of the privacy rights, a claim for violation of privacy in the workplace generally comes down to one factor: whether the employee had a reasonable expectation of privacy.

---

[16] *Id.*

[17] *See* American Management Association/ePolicy Institute, *2005 Electronic Monitoring & Surveillance Survey (2005)*, available at http://www.amanet.org/research/.

[18] *Id.* Further, employers have implemented policies governing email use (84%), personal Internet use (81%), personal IM use (42%), operation of personal Websites (34%) and personal blogs (20%) on company time, and personal posting on corporate blogs (23%).

Electronic Communications

The Electronic Communications Privacy Act of 1986 ("ECPA") amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The ECPA expanded the scope of Title III protection by including all electronic communications transmitted by wire, radio, electromagnetic, photoelectric, and photo-optic systems. Email communications are now, therefore, covered by Title III.[19]

It is likely that certain blogs will fall within the protections of the ECPA. If an employee is writing his or her blog on an employer-owned computer/server, or if the blog is hosted on an empoyer-owned server, then the act of writing may be held to be an electronic communication, and the ECPA could apply. However, research revealed no cases on point.

Two provisions of the ECPA, however, indicate that employer monitoring of electronic communications on the company's online computer system would not violate the Act. First, Section 2701 exempts the person or entity providing a wire or electronic communication service from liability for accessing stored private communications. Second, the ECPA allows an employer to disclose the contents of an employee's electronic communications if doing so is necessarily incident to retention of the service or to protect rights or property.[20]

California: Constitutional Right to Privacy

California, unlike other states, recognizes an employee's constitutional right to privacy in a private workplace. A 1972 voter initiative led to the adoption of a privacy protection clause in the state constitution. During the election campaign, supporters and opponents of the measure discussed the effects the clause would have on both government and business entities. In light of this unique legislative history, the California Supreme Court has construed the California Constitution to protect the state's residents against privacy invasions by public *and private* entities alike.[21] A plaintiff alleging an invasion of the state constitutional right to privacy must establish each of the following:

1) a legally protected privacy interest;
2) a reasonable expectation of privacy in the circumstances; and
3) conduct by defendant constituting a serious invasion of privacy.[22]

California courts have held that employees do not have a reasonable expectation of privacy in their email messages, provided they are given adequate notice. For example, in *Bourke v. Nissan Motor Corp.*,[23] the court found that the employees had no reasonable expectation of privacy, and thus their privacy rights were not violated, because they had signed a form detailing that the use of the company computers was for business purposes only. In *Flanagan v. Epson*,[24] an employee brought a class action lawsuit alleging that Epson invaded the employees' privacy by circumventing their passwords and reading their email messages while fostering an atmosphere which led them to believe their messages were private. The *Flanagan* court refused to extend California's right to privacy to employee email, suggesting that such a determination should be left to the legislature. Likewise, in *Shoars v. Epson America*,[25] a $ 75 million class action suit for invasion of privacy was dismissed, with the court observing that email privacy is in the province of the legislature.

A California court has further recognized that an employee lacks a reasonable expectation of privacy where he or she signs a policy acknowledging that computer use and communications were "not private."[26] In the *TBG* case, an employee sued his former employer for wrongful termination when it fired him for repeatedly accessing pornography over the Internet using employer-issued equipment. The employee had signed the employer's policy, agreeing not to use employer-issued equipment for non-business reasons unless specifically approved. He also agreed that TBG could monitor (including "review,

---

[19] Anyone can escape liability under the ECPA if one of the parties to a communication consents to an interception or disclosure of a message. 18 U.S.C. § 2511(2)(d) and § 2702(b)(3).

[20] *See* Fraser v. Nationwide Mutual Ins. Co., 135 F. Supp. 2d 623 (E.D. Penn. 2001) (determining that "interception" within the Wiretap Act and the Stored Communication Act did not include the action of the employer retrieving the employee's email message from post-transmission storage where the message remained after transmission was completed).

[21] *See* Hill v. National Collegiate Athletic Ass'n, 7 Cal. 4th 1 (1994) ("In summary, the Privacy Initiative in Article I, Section 1 of the California Constitution creates a right of action against private action, as well as governmental agencies.").

[22] *Id.* at 35-37.

[23] Available at http://www.loundy.com/CASES/Bourke_v_Nissan.html

[24] Cal. App. Dep't. Super. Ct. (1990) (no published decision).

[25] 1994 Cal. LEXIS 3670 (Cal. 1994) (no published decision).

[26] TBG Ins. Servs. Corp. v. Superior Court, 96 Cal. App. 4th 443 (2002).

copying, or deletion of messages, or the disclosure of such messages or files to other authorized persons") his computer use; that his communications transmitted over the equipment were "not private"; and that TBG could terminate him for misuse of the equipment. The employer sought production of the company-issued computer the employee had used at his home, and the employee objected that production would violate his right to privacy. The appellate court found the employer's policy defeated the employee's alleged reasonable expectation of privacy, although it permitted the employee to seek a protective order to protect personal information from disclosure.[27]

Common Law Privacy

The common law tort of invasion of privacy similarly focuses on an employee's "reasonable expectation of privacy." Before the emergence of electronically advanced forms of communication, courts analyzed an employee's expectation of privacy based on searches in the workplace. Thus, in *K-Mart Corp. Store No. 7441 v. Trotti*,[28] an employee successfully sued her employer for the tort of intrusion by establishing a legitimate expectation of privacy in her locker. K-Mart made lockers available to employees, but because locks were in short supply, it allowed plaintiff to provide her own lock and did not require her to furnish K-Mart with a combination or key. Acting on suspicion that a watch had been stolen and that price-marking guns were missing, K-Mart searched her locker contents (including her purse), without obtaining plaintiff's consent or even providing notice. The court found plaintiff enjoyed an expectation of privacy and that K-Mart had reinforced that expectation by allowing her to use her own lock.[29] The court then balanced the employee's expectation of privacy against K-Mart's business interests in controlling the locker, and held K-Mart's reasons for the search failed to justify the intrusion.[30] Moreover, the covert nature of the intrusion, without permission from the employee, contributed to the damages the employee suffered.[31]

This analysis has been extended to situations involving electronic communications. In *Smyth v. Pillsbury Co.*,[32] a plaintiff argued that his termination was wrongful because it was based on information obtained from email messages in violation of his right of privacy. The court rejected this argument stating, "Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."[33] This was true, despite the fact that the employer had repeatedly told its employees that all workplace email communications would be kept confidential. The court stated that even if the employee's privacy right were violated, "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[34]

Expectation: Identity and Computer Usage

While most blogs are publicly available such that an employee would have no reasonable expectation of privacy in the blog, monitoring an employee's access and changes to a blog stored on third-party equipment would likely raise questions of employee privacy. The courts have not addressed in any reported decisions the expectation of privacy that employees enjoy when accessing third-party servers where personal blogs are maintained. Some of these bloggers may believe that their true identities are shielded behind a user login name, and that their conduct (and discussion) cannot be attributed to them because of the anonymity. They may not realize, however, that commercially-available software allows employers to monitor, keystroke by keystroke, the text they type into these pages.[35] Further, such employees may not consider whether the third party may be forced, through technological or legal means, to identify the origin or author of the blog or the computer from which the text was posted.

Because employees may wish to access these services using their employers' computers and Internet connections, more likely than not, the courts will find that these communications are no more protected under anti-wiretap laws than electronic communications sent over a company's servers. However, to avoid any claims premised on a "reasonable expectation of privacy," employers should emphasize in their published Internet and computer policies that Internet usage and communications sent through or posted to third-party services by use of company equipment are equally subject to monitoring.

Finally, employers should be cautioned that their access to such third-party services is most likely

---

[27] *Id.* at 455.

[28] K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984).

[29] *Id.* at 638.

[30] *Id.* at 640.

[31] *Id.* at 640-41.

[32] Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

[33] *Id.* at 101.

[34] *Id.* at 101.

[35] *See, e.g.*, the publicity materials for the "Spector" software packages, available at http://www.spectorsoft.com.

limited to monitoring "real-time" data transmitted over their Internet connections. In a case decided in January 2001, the Ninth Circuit held that an airline violated the Electronic Communication Privacy Act (ECPA), when it accessed a disgruntled pilot's personal password-protected website – not maintained on a company computer – to read postings critical of management and the incumbent pilots' union.[36] The disgruntled pilot issued passwords only to non-management employees of the company. The company, therefore, asked a sympathetic employee to register for a password on the site; as part of the registration agreement, he promised not to disclose the contents of the site to third parties. He, of course, disclosed to the company various negative postings on the website, including one that (without any apparent basis in fact) stated that a senior executive was being investigated for fraud. The Ninth Circuit held that the company violated ECPA by making unauthorized access to the website.[37] Notably, the Ninth Circuit also held that the pilot was entitled to a trial on his claim that his anti-management postings were protected activity under the Railway Labor Act.[38]

Other Risks

Risks to Company Confidential and Trade Secret Information

California trade secret law and employee invention assignment and proprietary information agreements prohibit the unauthorized use or disclosure of an employer's trade secret and confidential information, regardless of whether the information is written in a book, used to create an invention, or posted to the Internet through a blog. Notwithstanding the many steps employers take to protect the secrecy of their information (and that of their customers and partners), blogs present a particular threat to the secrecy of confidential and trade secret information due to the informal nature of the communication, the ease of posting, and the broad access the Internet provides to such postings.

Intentional Disclosures of Company Information

One obvious threat is the possibility than an employee will intentionally disclose company information. For example, a disgruntled former employee might disclose his former company's confidential or trade secret information (such as an internal list of bugs in its product or a failed attempt to create a new feature in the product) as revenge for what the employee perceived as an unfair termination. Further, employees may disclose such information to gain popularity or make their blogs more interesting.

A recent "blogger" case may have arisen from such a disclosure. In *Apple Computer, Inc. v. Doe, et al*,[39] Apple sued unidentified individuals and entities for the alleged disclosure of Apple's confidential information about "a FireWire audio interface for Garage Band, codenamed 'Asteroid' or 'Q7.'" Websites, including Apple Insider and PowerPage, published this information. Apple subpoenaed Nfox, the email service provider for PowerPage, to obtain emails that might identify the source of the information. Jason O'Grady and two others ("O'Grady"), who self-identified as journalists but are more appropriately called "bloggers," moved for a protective order claiming a privilege from disclosing confidential sources and other protections. Ultimately, Judge James Kleinberg ruled that O'Grady's alleged privilege did not justify a protective order. Rather, where the at-issue subpoena involved allegedly misappropriated trade secret information and the publication of the information did not serve a "public interest," production of documents revealing the confidential source was appropriate. O'Grady appealed the decision, and the parties are briefing the matter.

Unintentional Disclosures of Company Information

Disclosures, however, need not be so obvious or intentional to result in damage to a company. For instance, an employee may discuss her work on her blog without identifying her employer, but nevertheless disclose confidential information. Or, an employee may post what he believes to be a funny or ironic fact or photo that the employer considers to be sensitive or even defamatory.

For example, in October 2003, Microsoft ended Michael Hanscom's temporary stint with Xerox at the Microsoft campus after Mr. Hanscom took a photo on the campus and posted it to his blog.[40] Mr. Hanscom, a longtime Mac fan, found the presence of stacked boxes of Apple Macintosh G5's on Microsoft's loading dock too funny to pass up. He took a picture of the boxes and posted it to his blog with the following caption: "Even Microsoft wants G5s." Microsoft indicated the posting was a security

---

[36] Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001), *opinion withdrawn*, 262 F.3d 927 (9th Cir. 2001).

[37] *Id.* at 1048.

[38] *Id.* at 1051.

[39] *See* Apple Computer, Inc. v. Doe 1, *et al.*, Santa Clara County Superior Court Case No. 1-04-CV-032178 (filed 12/13/04), Sixth Appellate District Case No. H028579 (appeal filed 03/22/05).

[40] *See* Jon Bonne, *Blogger dismissed from Microsoft: Copy shop worker loses position after posting Mac photo* (October 30, 2003), available at http://msnbc.msn.com/id/3341689.

violation and asserted that contractors were required to sign confidentiality agreements.

Disclosure of Customer and/or Partner Information
Under the prior examples, the employees would bear the liability for the unauthorized use or disclosure of confidential information; however, employees may also create liability for their employers by disclosing the confidential or trade secret information of the employer's customers or business partners. Thus, when analyzing the content of employees' blogs, it is important for companies to focus not only on protection of their own proprietary interests but those of third parties as well.

Blog Content May Negatively Impact Company Image
Even if the content of a blog does not give rise to legal liability (either to the employer or the employee), it may cast the company in an unfavorable light. And, readers may come across the blog without intentionally accessing it. For example, the content of such blogs may appear in the results generated by search engines. With more and more companies doing independent research on their customers, vendors, and business partners, an employee's blog may have the unintended effect of driving away customers before the company ever knows about the potential business opportunity.

Risks of Attempting to Prohibit Blogging

Even if an employee's blog does not implicate potential employer liability, an employer might nevertheless find an employee's blog objectionable based on its content. Acting on the objection could prove problematic.

Legal Risks
Lawful Conduct During Nonworking Hours
California's broad privacy laws protect employees from termination based on lawful off-duty conduct.[41] At first blush, it may seem that an employer has no legitimate interest in the content of an employee's personal blog, done using the employee's equipment on the employee's own time. However, an employer could face a dilemma when, for example, a company executive hosts a personal blog that is adamantly anti-gay marriage. Other employees, including gay employees, may see the blog and ask the employer to stop the postings. Or, perhaps the blog advocates white supremacy, and African-America employees see the blog and ask the employer to make the executive stop the postings.

In both instances, the employer may wish to step in and stop the blog, while at the same time harboring serious concerns about the executive's privacy rights. The right answer to the dilemma will depend on several factors, including the following:

- To what degree does the particular blog relate to the workplace? Does it reference the Company's name or other identifying information? Is the blogger a high-profile employee whom the reader will likely associate with the Company? Or, is the reader likely to believe that the person, because of his position, expresses a Company view?
- In the Company's opinion, how offensive is the content of the blog? (Does the blog express an opinion on a particularly sensitive social issue? While the Company may not agree with the particular viewpoint, is it well-expressed or inflammatory?)
- How likely is it that such a statement will create legal liability for the Company? (For instance, is it harassing in nature?)
- Does the blogger have a reasonable expectation of privacy?
- Do Company core values so conflict with the content of the blog that the Company feels it must stop the blog or terminate the employee?

In the case of a well-articulated, but debatable position, the Company will less likely be able lawfully to stop the blog and/or terminate the employee. However, an inflammatory message touting white supremacy, which uses offensive epithets and can somehow be traced back to the Company, likely would justify Company action. The tougher calls, of course, fall in between.

Political Activities
California Labor Code sections 1101 and 1102 expressly protect an employee's right to engage in political activities by prohibiting employers from (1) interfering with employees' political activities or (2) coercing (or attempting to coerce) employees "to adopt or follow or refrain from adopting or following any particular course or line of political action or political activity." Thus, in determining whether a company can request that an employee stop a blog or discipline an employee for not doing so, the company must be sensitive to nuances in the blog content that may give rise to a claim under Sections 1101 or 1102.

Returning to the example of the executive with a blog advocating white supremacy, if the executive posts proposed legislation he advocates for achieving goals of white supremacy, and requests his readers participate in his grassroots campaign to get the

[41] *See* Cal. Lab. Code § 96(k).

legislation passed by signing a petition, an attempt to shut down the blog could violate his rights to express his political views as well as his privacy rights. Such situations require a very careful balancing of competing rights and recognition that there may be some legal risk posed no matter how the company responds. In such cases, the employer may decide to pursue the option with the smallest legal risk or the option that is most consistent with the company's values, regardless of legal risks.

Concerted Activity

Section 7 of the National Labor Relations Act ("NLRA") protects employees' rights to engage in "concerted activity for the purpose of . . . mutual aid and protection."[42] Employers that interfere with these rights may violate Section 8(a)(1) of the NLRA.[43] These rights are *not* limited to the union setting; rather, employees enjoy Section 7 rights whether or not they are part of a union labor force.

The National Labor Relations Board ("NLRB") has recognized that electronic communications (in particular, email) can qualify as concerted activity. In *Timekeeping Systems, Inc.*,[44] the NLRB determined that a company violated the rights of its white-collar, non-unionized employees to engage in "protected concerted activity" when the employer terminated an employee for comments made on the company email system. The company's Chief Operations Officer had sent an email to employees soliciting their input on a proposed vacation and bonus plan. One employee hit the "reply all" button, sending his response to his manager and all recipients of the manager's email, and in a "flippant and rather grating" email identified several problems with the proposed changes. The Administrative Law Judge held that the email was sent for the "purpose of mutual aid and protection," notwithstanding its tone, and was therefore protected under Section 7 of the NLRA.[45] The judge rejected the employer's argument that the computer system had been disrupted by the email, noting that the employer routinely allowed personal email and telephone usage.[46] The NLRB affirmed the order requiring reinstatement and back wages.[47]

In an earlier case, the Board held that a company could not prohibit the use of company computers to distribute union announcements when the company had (1) allowed personal use of the system, and (2) encouraged members of a company-sponsored labor-management committee to use the email system.[48]

What does this mean for employers? As to corporate-sponsored blogs, an employer that permits employees to express personal opinions and convey non-business information in such blogs should be cautious about disciplining employees for the content of blogs geared at labor organizing or other arguably protected activity (such as criticizing management, raising safety concerns, or comparing compensation). As to personal blogs, to the extent an employer permits employees to use company equipment for non-business purposes (for instance, to check a personal email account or surf the Internet), an employer should similarly be cautious about disciplining employees for labor organizing or other arguably protected activity based on the content of the blog or on the employee's use of company resources to update the blog.

Which Approach to Blogging is Best?

That depends. Determining a company's official position on employee blogging is a much harder task than it appears at first glance. At the end of the day, settling on a "blog philosophy" requires a company to do a self assessment to determine what balance between technological savvy, forthright communication, and legal risk best fits with the corporate culture and image the company wishes to maintain.

*****

Shawna M. Swanson is the partner leading Fenwick & West LLP's San Francisco-based Employment Practices Group. Ms. Swanson litigates employment cases, provides counseling to employers, and regularly trains managers and employees on various employment law topics, with a special emphasis on preventing and investigating claims of unlawful harassment and discrimination. Ms. Swanson graduated with honors from Harvard Law School in 1993.

---

[42] 29 U.S.C. § 157 et seq.

[43] 29 U.S.C. § 158(a)(1).

[44] 323 N.L.R.B. 244 (1997).

[45] *Id.* at 248 (adopting and attaching ALJ's decision).

[46] *Id.* at 249.

[47] *Id.* at 245.

[48] *See* E.I. du Pont de Nemours & Co., 311 NLRB No. 88 (1993). However, in analogous cases involving telephones, bulletin boards, and videocassette players, the Board has upheld evenhanded restrictions on non-business use of company property to disseminate messages, even if they effectively bar the union from accessing those resources. *See, e.g.*, Mid-Mountain Foods, Inc., 332 NLRB No. 19 (2000) (employer did not violate NLRA when it did not allow union to show organizing video on VCR in employees' break room; no evidence that employees were allowed to play personal videos or that company had shown anti-union videos).

Patrick Sherman is an associate in Fenwick & West LLP's Mountain View office. A member of the firm's Employment Practices Group, Mr. Sherman focuses his practice on employment litigation and counseling. Mr. Sherman is a 2003 graduate of Duke Law School.

Any reader interested in sharing information of interest to the labor and employment bar, including notices of upcoming seminars or newsworthy events, should direct this information to Michael C. Sullivan, 401 B Street, 10th Floor, San Diego, CA 92101, Fax: (619) 615-0700, email: msullivan@paulplevin.com, or Wendi Reed, Practice Area Editor, Matthew Bender & Co., email: Wendi.Reed@lexisnexis.com.