

Law Report

LEGAL NEWSLETTER

VOLUME 7, ISSUE 2

MONITORING ELECTRONIC COMMUNICATION IN THE WORKPLACE

While employees hold strong rights to maintain their private lives without intrusion, employers can legitimately place limits on the use of workplace Internet access or email facilities for activities unrelated to company business. Confronted with this potential conflict between worker rights to privacy and company prerogative to regulate the work environment, California courts have provided useful policy guidelines that should keep upsets and legal claims arising from this sensitive area to a minimum.

The California Supreme Court specifies three steps for an employee to establish a constitutionally prohibited invasion of privacy

CALIFORNIA PRIVACY RIGHTS IN THE WORKPLACE

California Constitution, Article I, Section 1 protects all workers in this state: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty,

acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

The California Supreme Court specifies three steps for an employee to establish a constitutionally prohibited invasion of privacy:

(1) existence of a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of his/her privacy. *Hill v. National Collegiate Athletic Association*, (1994) 7 California Reports 4th (Cal.4th)1, 26 California Reporter 2d (Cal.Rptr.2d) 834.

In *TBG Insurance Services Corporation v. the Superior Court of Los Angeles County*, (2002) 96 California Appellate 4th (Cal.App.4th) 443, 117 California Reporter 2d (Cal.Rptr.2d) 155, Court of Appeal applied these three steps in the workplace context with perhaps surprising results.

Employer TBG terminated executive Robert Zieminski for violating the company's electronic usage policy by accessing pornographic web sites at work. Zieminski sued TBG for wrongful termination, alleging that the pornographic sites found on his work computer had "popped up" on his workplace computer involuntarily and that the

real reason he was fired was to prevent his stock options from vesting.

Employer TBG terminated executive Robert Zieminski for violating the company's electronic usage policy by accessing pornographic web sites at work

TBG had previously provided Zieminski with two company computers, one for use at work, the other for company use at home. On receipt of this equipment, Zieminski had signed TBG's policy agreeing (a) to use both computers only for business purposes and not for personal benefit; and (b) to refrain from using these computers and related equipment for obscene or other inappropriate purposes. Before trial, TBG asked the court to compel him to disclose information from the home computer so that TBG could determine whether Zieminski had accessed similar pornographic websites at his home in violation of the above policy. Zieminski claimed TBG had no right of access since that home

computer contained personal information and disclosure would invade his constitutional privacy rights.

Although the trial judge denied TBG access to that home computer, the Court of Appeal disagreed, ruling that the signed and agreed-upon policy established that Zieminski did not have a reasonable expectation of privacy when using that home computer, even though he used it partially for purely personal matters. In deciding in favor of the employer's access to that home computer, the Court of Appeal recognized: (i) accepted community norms regarding use of company computers, including the accepted rights of employer access to data bases on such

Please see "MONITORING" page 2

SEXUAL HARASSMENT SEMINARS

Employment Law Seminars Available for All Employers

Visit our website at www.tbowleslaw.com to find times & schedules of our current seminars

The Law Offices of Timothy Bowles work primarily in employment and health care fraud law; mediation; arbitration; and civil litigation. While published articles convey the firm's views on topics it has found concern many of its clients, the articles are not intended and should not be considered legal advice. Such professional advice requires full disclosure to an attorney of a client's circumstances and that attorney's opportunity to analyze those circumstances against applicable law.

LAW OFFICES OF TIMOTHY BOWLES, P.C.

ONE SOUTH FAIR OAKS AVE., SUITE 301, PASADENA, CA 91105 • TELEPHONE: (626) 583-6600 • FAX: (626) 583-6605
tbowles@tbowleslaw.com • www.tbowleslaw.com

LAW OFFICES OF TIMOTHY BOWLES, P.C.

ONE SOUTH FAIR OAKS AVE., SUITE 301
PASADENA, CA 91105

ADDRESS SERVICE REQUESTED

Prsrt. Std
U.S. Postage
PAID
Glendale, CA
Permit No. 61

IN THIS ISSUE

*Monitoring Electronic
Communication in
The Workplace*

*New Attorney
Joins Our Firm*

“MONITORING” Continued from page 2

equipment; (ii) the existence of advance notice to Zieminski of Company’s electronic policy statement; and (iii) Zieminski’s opportunity to consent or not consent to Company’s policy statement. The court concluded that within the modern-day employment context, workers do not enjoy unrestricted expectations of privacy in their use of company-issued computers. Since TBG gave Zieminski advance notice of its electronic policy statement and as Zieminski consented to that policy in writing, TBG was able to access that home computer.

RECOMMENDATIONS FOR COMPANY COMPUTER PRIVACY POLICIES

The Court of Appeal specified that employers can reasonably define and limit employees’ reasonable

expectations of privacy by having clearly stated policies. The court recommended that company computer-related privacy policies include:

*The Court of
Appeal specified
that employers can
lessen employees’
reasonable
expectations of
privacy by having
clearly stated
privacy policies*

- (1) electronic communications on company equipment are to be limited solely to business purposes;
- (2) employer reserves the right to monitor or access office internet or email usage;
- (3) the employer will keep copies of internet or email

- passwords;
- (4) the existence of internet or email passwords does not mean the communications are confidential;
- (5) a statement forbidding the transmission of discriminatory, offensive or unprofessional messages;
- (6) access to discriminatory or offensive websites is strictly prohibited; and
- (7) employees are forbidden from posting personal opinions on the Internet using company access.

CONCLUSION

Employers should provide their workforces with clearly worded electronic equipment data storage and communication policies specifying the acceptable and intended uses for workplace computers and reserving the employer’s right to inspect and monitor employees’ usage of such systems. We can assist employers on such policies or to answer questions on electronic communication monitoring protocols. ■

LAW OFFICES OF TIMOTHY BOWLES, P.C., IS PLEASED TO ANNOUNCE CYNTHIA S. BAMFORTH HAS JOINED THE FIRM AS AN ASSOCIATE

Ms. Bamforth is a 1988 Wesleyan University graduate. She received her 1996 Seattle University School of Law degree magna cum laude. A member of the State Bar of California since 1997, Ms. Bamforth comes to the firm after four years as vice president and corporate counsel for an Internet-based company.