

EMPLOYERS MUST USE CAUTION WHEN RELYING UPON THEIR “COMPUTER AND ELECTRONIC COMMUNICATIONS USE POLICY” TO REVIEW CONTENT ON THEIR EMPLOYEES’ COMPUTERS

By Clifford S. Anderson, Esq.

The “information age” poses unique challenge for employers trying to manage the “electronic workplaces” of their employees to ensure no violations of company policy (e.g., prohibitions on unproductive time surfing the internet, sending improper emails, etc.). These challenges include the intersection between the right of employers to review all communications of their employees over employer-owned computers and the right of employees to privacy with regards to *personal* communications that they might happen to send using employer-owned computers. When an employer suspects employee wrongdoing and/or an employee ends employment, and subsequent litigation is a possibility, the intersection of these issues becomes even more important. In such situations, the employer must exercise appropriate care when examining its employees’ company-owned computers.

Unsurprisingly, the starting point for determining the scope and procedure for any review of an employee’s work computer is to first review the employer’s “Computer and Electronic Communication Use Policy.” Any employer who does not have such a policy should put one in place. Such policies typically include provisions that state, among other things: (1) that email and computer systems belong to the employer; (2) that personal email messages sent or received on company-owned computers may be reviewed for legitimate business purposes and

that there is no expectation of privacy; (3) that the employer reserves the right to access and disclose documents, Internet logs, programs, and other files and information contained on and saved in the employer’s computer systems; (4) that e-mail messages and employee use of computer systems may be monitored by the employer to the extent necessary to ensure compliance with company policies; and (5) that the creation, display, transmission, receipt, or storage of sexually explicit or pornographic messages, images, cartoons, or any documents, programs, or files, or any transmission or use of e-mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassing, threatening, or disparaging is prohibited.

Notwithstanding wide-spread use of such policies, employers should be careful regarding how such policies are actually implemented and utilized. While on their face, such well drafted policies would seem to give employers *carte blanche* to review “every electronic move” of their employees, the reality, is they do not. Thus, blind reliance on such policies by employers can have negative unintended consequences that can be costly and problematic, particularly, if litigation arises. Contrary to conventional wisdom, recent court decisions reveal that even well-crafted electronic communication policies do not allow unfettered exploration and scrutiny of an employee’s “cyber life.” Those decisions also suggest that it may be time for employers to revisit the language of their policies for possible improvements and to re-examine how; in fact, employers are actually utilizing and implementing their policies to reduce the chance of unintended consequences that can arise from blithely undertaking reviews of employee communications without careful thought and planning.

Recent court decisions have focused on the following typical fact pattern. An employee seeks personal legal advice, often in connection with a possible termination of her employment. Yet, she carelessly begins communicating with her attorney using the employer’s email system. Sometimes, the employee utilizes the employer’s computer but accesses her personal Yahoo or Gmail account, for example, to communicate with her lawyer. In either case, the following sticky questions arise: (1) are such

communications protected by the attorney-client privileged or is the privileged waived by the employee due to her agreeing to the employer’s electronic communications policy? (2) if such communications are protected, and the employer nonetheless reviews them, what are the consequences, especially if there is litigation?

With regards to the first question, recent cases mostly hold such communications are privileged. The most protected communications are those sent by employees using their *personal* email accounts such as Yahoo or Gmail, but, nonetheless, doing so using the employer’s computers. See, e.g., *Stengart v. Loving Care Agency, Inc.*, 408 N.J. Super. 54, 973 A.2d 390 (Sup. Ct. NJ 2009) (finding no waiver of attorney-client privilege of Yahoo email communications sent by employee on company-owned laptop); *Nat’l Economic Research Associates, Inc. v. Evans, et al.*, 2006 WL 2440008 (Mass. Super. Ct. August 3, 2006) (same); and *Curto v. Medical World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (no waiver of attorney-client privilege for emails to counsel sent by employee through her personal email account on a company-owned computer used in her home). But see *Long v. Maurbeni Am. Corp.*, 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006) (finding waiver with private password-protected email accounts).

The decisions are more mixed where the attorney-client communications are sent over the employer’s own email system or where the privileged information ends up residing on the hard drive of the employer-owned computers. Nevertheless, many courts have still held such communications to be privileged. See, e.g., *United States v. Hatfield*, 2009 WL 3806300

(E.D.N.Y. Nov. 13, 2009). See also *Fiber Materials, Inc. v. Subilia*, 974 A.2d 918 (Sup. Jud. Ct Me. 2009) (dismissing interlocutory appeal on technical grounds but chastising employer’s lawyers who reviewed ostensibly attorney-client privileged communications of former employee and included information from such communications in its complaint). On the other hand, a few courts have held the attorney-client privilege to be waived when company email systems are used. See, e.g., *Scott v. Beth Israel Medical Center, Inc.*, 847 N.Y.S.2d 436 (Supreme Ct. N.Y County NY 2007) (emails using employer’s computer system and employee’s email address at work) and *Kaufman v. SunGard Invest. Sys.*, 2006 WL 1307882 (D.N.J. May 10, 2006) (emails sent and received on company’s email system).

With regards to question two above, the cases teach that, notwithstanding solid electronic communication policies, there are, nonetheless, risks in an employer and/or its counsel accessing privileged documents found on an employee’s company computer. One risk is that, even before litigation, key decision makers may inadvertently learn about a disgruntled employee’s communications with counsel about bringing possible litigation against the employer even *before* a planned termination decision has been implemented. Such facts make it much more difficult for the employer to proceed with a planned and legitimate termination without raising the specter that the discharge is retaliatory due to the employer’s knowledge of the employee’s contemplated suit against the employer.

An even more significant risk is disqualification of the employer’s counsel in any subsequent litigation. In this scenario, the privileged communications are unwisely shared with counsel thus tainting their ability to continue as the employer’s counsel. Disqualification in this situation can be particularly damaging especially after significant legal fees have been expended and counsel has developed substantial knowledge about the case.

In analyzing the degree to which employers may review their

employee’s electronic communications, courts “have sought to determine whether the employee, as a practical matter, had a reasonable expectation that the attorney-client communications would remain confidential despite being stored on a company’s computer system.” *Hatfield*, 2009 WL 3806300 at *8. To evaluate this issue, courts examine the following five factors: (1) whether the employer maintains “a policy banning personal or other objectionable use?” (2) whether the employer monitors “the use of the employee’s computer or e-mail?”; (3) whether third parties “have a right of access to the computer or e-mails?”; (4) whether the employer notified its employee, or “was the employee aware, of the use and monitoring policies?” and (5) how does the employer interpret its own policy regarding its right to privileged information? *Id.*

The above factors, and the cited cases, suggest the following practice pointers to avoid the risks identified above when reviewing an employee’s employer-owned computer:

- (1) Add language in your electronic communications policy that expressly prohibits employees from using their company computers to conduct personal legal business;
- (2) Add language in your electronic communications policy that states that employees should use their own computers and own personal email accounts for *confidential* personal business;
- (3) Be sure employer’s electronic communications policy is circulated broadly and make known that IT staff is permitted, at any time, to conduct random checks of company-owned employee computers;
- (4) If a problem employee is identified for which a review of her electronic communications is required, have company “neutrals” separate from the employee’s immediate supervisor first receive a report on what is found in order to insulate decision makers from being tainted with potentially privileged information communicated by the employee;
- (5) If the “neutral” team discovers privileged communications, train that team how to handle such circumstances. Such steps might include, without disclosing the contents of such communications, seeking legal advice from the employer’s counsel regarding how to handle the discovery of such information. Doing so will avoid the potential for disqualification of the employer’s counsel in any subsequent litigation; and
- (6) If necessary, utilize separate counsel, different from the attorney team that might be involved in litigation with the employee at issue, to provide advice regarding how to handle the potentially privileged information. This too will reduce the risk of disqualification.

The reality of the information age is that employees will always continue to use their work computers for limited personal uses. Such uses will inevitably include, occasionally, careless communications by employees with their lawyers representing them in possible litigation against their employers. Implementation of the above practice pointers will, however, help minimize the risk of the adverse unintended consequences that may arise upon an employer stumbling across privileged communications.

ELECTRONIC NEWSLETTERS

If you would like to receive our newsletters electronically, please send us your e-mail address at marketing@hjlawfirm.com

This newsletter provides general information on legal matters, and should not be relied upon as legal advice. A qualified attorney must analyze the relevant facts and apply the applicable law to provide specific legal advice. If you require legal advice or want additional information regarding the services we offer, please contact Cliff Anderson, Esq. at csanderson@hjlawfirm.com or Karl Robinson, Esq. at krobinson@hjlawfirm.com, or both can be reached at 952-941-4005.

INDEPENDENT CONTRACTOR ISSUES CONTINUE TO BE IMPORTANT IN 2010

By Karl E. Robinson, Esq.

With businesses of all sizes looking to save money in these challenging economic times, one common but potentially risky cost-cutting measure is using independent contractors rather than employees. Using independent contractors can provide savings in income tax withholding, unemployment and workers' compensation insurance contributions, overtime, and employee benefits. Also, some antidiscrimination laws may not apply to independent contractors, since typically such laws apply to "employees."

Companies should be aware, however, that if they classify a worker as an independent contractor when the individual is really an employee, they may face significant legal liabilities. For example, a worker misclassified as an independent contractor may be entitled to overtime wages and other benefits, and the employer could face civil penalties and other sanctions. Employers could also face unexpected

unemployment insurance liability, back taxes, or other penalties based on the misclassification.

In Minnesota, courts normally examine five factors to determine whether an individual is an independent contractor or an employee: (1) the right to control the means and manner of performance; (2) the mode of payment; (3) furnishing of materials and tools; (4) control of premises where work is performed; and (5) right of the employer to hire and fire. *See, e.g., C.B. ex rel. L.E. v. Evangelical Lutheran Church in America*, 726 N.W.2d 127, 133 (Minn. Ct. App. 2007).

Accordingly, businesses should be careful in how they are using the independent contractor classification for their workers. Companies that simply rely on industry standards, boilerplate independent contractor agreements, or a representation by the worker that he or she is an independent contractor may be risking exposure to significant legal liability. It is therefore advisable to discuss these independent contractor issues with an attorney.



HELLMUTH & JOHNSON PLLC
ATTORNEYS AT LAW

10400 Viking Drive, Suite 500
Eden Prairie, Minnesota 55344

PRSR STD
US Postage
PAID
Minneapolis, MN
PERMIT 4656

THE AUTHORITY

EMPLOYMENT LAW

WINTER 2009 - 2010

THE NEWSLETTER FOR CLIENTS AND FRIENDS OF
HELLMUTH & JOHNSON PLLC

10400 Viking Drive, Suite 500
Eden Prairie, MN 55344
T 952-941-4005 F 952-941-2337
www.hjlawfirm.com

FOR PAST NEWSLETTERS,
ARTICLES AND ADDITIONAL
INFORMATION:
HJLAWFIRM.COM



H&J ATTORNEYS NAMED TO 2010 MINNESOTA RISING STAR® LIST

Recognized Among top 2.5% Attorneys in State

Hellmuth & Johnson, PLLC announced that Minnesota Law & Politics magazine has named four firm attorneys to the 2010 Minnesota Rising Star® list. The attorneys were recognized in the December 2009 issues of Minnesota Law & Politics, Twin Cities Business and Mpls/St.Paul Magazine.

The attorneys named to the 2010 list are: Matthew J. Franken, Joel A. Hilgendorf, Christopher R. Jones, and Anthony T. Smith.

Representing the top 2.5 percent of attorneys in the state as selected by their peers, the "Rising Star" list recognizes the accomplishments of attorneys who have practiced for 10 or less years and are 40 years of age or younger.

To learn more about the "Rising Stars", we invite you to visit their biographies on our website at www.hjlawfirm.com.

H&J ADDS NEW ATTORNEYS

Please help us welcome the following attorneys:

Gary Fuchs joins us as a Partner practicing in real estate law, construction and civil litigation, eminent domain and mediation/arbitration.

Raymond Bonnabeau joins us as a Partner practicing in information technology and eCommerce.

Elizabeth Rein joins us as an Associate practicing in real estate law, construction and litigation.

Susan Anderson joins us as an Associate practicing in estate planning and trust law.

You can learn more about them at www.hjlawfirm.com