WSGR ALERT

MARCH 2011

IN SEXUAL HARASSMENT CASE, CALIFORNIA COURT OF APPEAL UPHOLDS EMPLOYER'S INSPECTION AND USE OF EMPLOYEE'S PERSONAL EMAILS

Holmes V. Petrovich Development Company, LLC

In today's workplace, employers periodically consider whether—and under what circumstances—they may inspect employee emails. The issue may arise in the context of a sexual harassment investigation, concerns that an employee has compromised company trade secret information, workplace safety threats, or many other potential inquiries into workplace misconduct matters. While employers commonly believe that an employee has no expectation of privacy with respect to email created using a company's computer, stored on its network, or sent or received using a company-supported email or messaging system, legal issues do exist. A well-drafted company policy improves an employer's odds in defeating an employee's assertion that he or she enjoys a right to privacy in "personal" email in the workplace. A recent case, *Holmes v. Petrovich Development Company, LLC,* provides further guidance for employers on how to maximize their discretion to inspect employee emails should they desire to do so.

In *Holmes*, a California Court of Appeal faced the question of whether an employee had a reasonable expectation of privacy in personal emails sent to her attorney via her employer-provided email account and using its computer. As discussed below, the court held that the employee did not have a reasonable expectation of privacy due, in large part, to the employer's strict technology resources policy. The case is instructive with respect to the effect that an electronic resources policy can have on an employer's right to access and inspect an employee's emails.

Underlying Lawsuit

The *Holmes* case was brought by Gina Holmes, an executive assistant, who resigned her position after exchanging a series of emails with her employer, Petrovich Development Company, regarding Holmes' pregnancy and upcoming leave of absence. Before Holmes left the company, she emailed an attorney about the situation from a company computer using her company email account. When Holmes filed a lawsuit against Petrovich alleging sexual harassment, retaliation, wrongful termination, violation of the right to privacy, and intentional infliction of emotional distress, the company accessed and inspected Holmes' email account and discovered the emails sent to her lawyer. When Holmes learned that Petrovich had the emails, she demanded their return, contending that they were privileged attorney-client communications. The company nevertheless used the emails at trial to show that Holmes did not suffer severe emotional distress and that she filed her harassment lawsuit only after her attorney urged her to do so. The company prevailed at trial, and Holmes appealed, arguing, among other things, that the trial court erred in allowing the company to use the emails Holmes sent her attorney.

Sexual Harassment Rulings

The court quickly dispensed with Holmes' sexual harassment, constructive discharge, and retaliation claims before engaging in a lengthy discussion of Holmes' privacy claims. In doing so, it applied familiar law governing sexual harassment claims. First, the court ruled in favor of the company on Holmes' hostile work environment claim, reiterating that sexual harassment laws do not constitute a general civility code. The court also held that Holmes could not prevail on her constructive discharge claim since she failed to establish the existence of a hostile work environment. Finally, the court rejected Holmes' retaliation claim, finding that the mere fact that Holmes' boss forwarded Holmes' email containing sensitive personal information to others in the office was insufficient to constitute an adverse employment action.

Effect of Electronic Resources Policy on Employees' Reasonable Expectation of Privacy

The law appears fairly settled that private employers can review employee email communications stored on company servers when the employer has provided notice of such monitoring, typically though an electronic resources policy. Recently, in *City of Ontario v. Quon* (http://www.wsgr.com/WSGR/Display.aspx?

Continued on page 2...

In Sexual Harassment Case . . .

Continued from page 1...

SectionName=publications/PDFSearch/wsgralert_employee_text_messages.htm), the United States Supreme Court suggested that the City of Ontario's computer usage policy, and therefore the ability of the city to monitor and audit employee communications, extended to the messages sent and received on Quon's employer-issued pager because the city clearly established the extension of the policy to the pagers. The Supreme Court also noted that "[t]he operational realities of the workplace . . . may make some employees' expectations of privacy unreasonable" and further noted that "[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." In *Holmes,* the employee asserted that whatever Petrovich's policy stated, she nevertheless had a reasonable expectation of privacy in her emails because the "operational reality" of her workplace was that her employer did not access or audit employee computer usage.

The *Holmes* court rejected that argument, and also noted that *Quon* was a public-sector case, not one dealing with a private employer. Also, the court specifically noted that Petrovich's employee handbook contained a technology resources policy warning employees that the company email account was to be used only for company business and not personal matters, that emails were not private, and that the company periodically would monitor its technology resources to ensure compliance. The policy specifically stated that email should be regarded as a postcard rather than a sealed letter because its contents could be viewed. Holmes agreed to the policy by signing the handbook acknowledgment, and she did not contend that Petrovich conveyed any conflicting messages regarding privacy expectations. Thus, in effect, the court determined that because of the policy in question, the "operational reality" of this workplace was that employees such as Holmes simply did not have a reasonable expectation of privacy in emails sent to others from her company email account on her company computer.

As to the emails Holmes sent to her attorney, the court essentially concluded that the lack of any expectation of privacy stripped the emails of any protection under the attorney-client privilege. In the court's view, the emails Holmes sent to her attorney were not protected by the attorney-client privilege because the communications did not represent a "confidential communication" between a client and a lawyer under applicable California law as they were "not transmitted 'by a means which, so far as the client is aware, discloses the information to no third persons other than those who are present to further the interest of the client in the communication." In so concluding, the court said that Holmes emailing her attorney from her company account and computer was akin to Holmes "consulting her attorney in one of [Petrovich's] conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by Petrovich would be privileged." Such a communication, the court said, was not privileged.

Ability of Employer to Retain Access Rights to Company-Provided Electronic Resources

Holmes helps further establish that a carefully drafted electronic resources policy coupled with a consistent practice of enforcement would do the most to bolster an employer's argument that it has a right to access and inspect employee email. *Holmes* also suggests that a well-drafted electronic resources policy standing on its own (and without conflicting messages or statements as to employee privacy) will go far in defeating any employee expectation of privacy and strongly supports an employer's right to access and inspect company emails, even if personal, and *regardless of the company's actual practice of enforcing the policy*.

For a variety of legitimate business purposes, an employer may elect to accommodate cultural concerns and avoid stating flatly that it has an unequivocal right to examine employee email. In striking that balance, however, that employer should do so knowing that it may be elevating the risks associated with inspecting employee emails at its discretion. In *Holmes*, where the employer was clear that it retained the right to inspect employee emails, it was easier for the court to determine that the employee enjoyed no expectation of privacy in her emails, even those sent to her attorney. Although this solution (i.e., making perfectly clear that employees enjoy no expectation of privacy in their company email) may not be desirable or practical for all employers, it is worth considering. Furthermore, as this area of law continues to evolve, employers should continue to assess the adequacy of their policies in protecting company interests.

If you need assistance creating or updating your electronic resources policy or have questions regarding employee email access, please contact an attorney in Wilson Sonsini Goodrich & Rosati's employment law, media, or consumer regulatory and privacy practices.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on March 11, 2011. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com