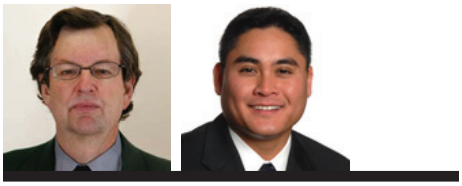
THE RECORDER

134RD YEAR NO. 10 www.therecorder.com FRIDAY, APRIL 1, 2011

Communication With Counsel Not Always Private



Fred M. Blum and Antonio P. Garcia Jr.

Your largest corporate client's president calls you to complain that she has a huge headache. She informs you that an employee allegedly received emails from a supervisor in which she was asked out on a date. Now, the employee is suing the company for sexual harassment.

During the workup of the defense, your hardworking associate finds that prior to filing suit, the employee emailed her attorney using your client's computer. The emails indicate that the employee actually went on the date, had a lovely time, and wanted to marry her supervisor.

Can you use this powerful evidence? Or will your possession of it cause the employee to accuse you of invading her attorney-client privilege? A recent California court of appeal case provides the answers concerning when the employee's communications are admissible, and how employers can protect themselves against employee privacy claims.

'HOLMES' AND EMPLOYEE EMAILS

In *Holmes v. Petrovich Development Company, LLC*, 11 C.D.O.S. 560, the Third District Court of Appeal defined when an employee's use of her employer's email system is protected and when her privacy rights, including the attorney-client privilege, are waived. Holmes claimed that her employer, Petrovich, harassed her due to her pregnancy. Prior to filing suit, Holmes communicated with her boss and apparently resolved the matter. However, she later emailed her attorney to describe the alleged harassment and expressed an interest to sue Petrovich. After meeting with her attorney, Holmes resigned and sued Petrovich for, among other things, sexual harassment and intentional infliction of emotional distress.

Petrovich had an explicit company policy regarding electronic communications. The employee handbook stated that "the company's technology resources should be used only for company business and that employees are prohibited from sending or receiving personal emails." The handbook also stated that "employees who use the Company's Technology Resources to create or maintain personal information or messages have no right to privacy with respect to that information or message." Petrovich reserved the right to "inspect all files or messages ... at any time for any reason at its discretion" and that it would "periodically monitor its technology resources for compliance with the company's policy."

At trial, Petrovich attempted to introduce Holmes' emails to her attorney as evidence that she did not suffer any emotional distress. Holmes moved to preclude Petrovich from introducing the emails because they were attorney-client communications. In denying Holmes' motion, the trial court noted that the emails were not private because she used Petrovich's computer to send the emails to her attorney. On appeal, the Third District affirmed.

NO EXPECTATION OF PRIVACY, THEN NO PRIVILEGE

The appellate court noted that Evidence Code §917 provides that a communication between persons in an attorney-client relationship "does not lose its character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication." However, "this does not mean that an electronic communication is privileged (1) when the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions."

The court reasoned that when Holmes emailed her attorney, she did not use her home computer. If she had, the communication would still be privileged because only unknown persons who were involved in the "delivery, facilitation, or storage" would have access to the email. Instead, Holmes used Petrovich's computer, "after being expressly advised this was a means that was not private and was accessible by Petrovich, the very person about whom Holmes contacted her lawyer and whom Holmes sued." As the court pointed out, "[t]his is akin to consulting her attorney in one of the defendants' conference rooms, in a loud voice, with the door open." Because the use of Petrovich's computer would expose the emails to her employer, Holmes waived the attorney-client privilege with her communications.

OPERATIONAL REALITY

Holmes argued that, despite Petrovich's computer use policy, she still had a reasonable expectation of privacy regarding her emails because the operational reality was that Petrovich did not regularly access or audit the employees' computers. Holmes relied upon *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), *rev'd, City of Ontario v. Quon*, ___ U.S. ___ (2010), in which the Ninth Circuit U.S. Court of Appeals held that a police sergeant who sent private text messages from an employer-issued text pager had

Fred M. Blum and Antonio P. Garcia Jr. are partners in the San Francisco firm of Bassi, Edlin, Huie & Blum.

a reasonable expectation of privacy in his text messages due to the "operational realities of the workplace." The Ninth Circuit found that despite a department policy stating that users of pagers had no right to privacy, the operational reality was that *Quon* was given a message to the contrary by his supervisor.

The Third District found that *Quon* was distinguishable. *Quon* involved a government employer and relied heavily on *O'Connor v. Ortega*, 480 U.S. 709 (1987), in which the Supreme Court held that "the fact an employee works for the government does not negate the employee's Fourth Amendment right to be free of unreasonable governmental searches at work." However, the Supreme Court noted that "the operational realities of the workplace ... may make some employees' expectations of privacy unreasonable." Although each employee's expectation of privacy should be decided on a case-by-case basis, "the existence of specific office policies, practices, and procedures may have an effect on public employees' expectations of privacy in the workplace."

The Third District found that even if the operational reality test applied, Petrovich had an explicit company policy that employees did not have a right to privacy in their emails and never conveyed any conflicting policy. The court noted: "Absent a company communication to employees explicitly contradicting the company's warning to them that company computers are monitored to make sure employees are not using them to send personal email, it is immaterial that the 'operational reality' is the company does not do so." Hence, it was unreasonable for Holmes to conclude that her emails would be treated by the company as private.

WHAT EMPLOYERS MUST DO AFTER 'HOLMES'

Holmes established a simple legal test concerning the admissibility of employee emails generated from an employer's server: An electronic communication to one's attorney is not privileged if the employer informs the employee that the email would not be treated as confidential and the employer can view the email. However, this simple concept serves as a powerful tool for employers who end up in litigation with their employees.

Holmes demonstrates that personal use of an employer's technology resources may be used against employees who file claims against the employer. In *Holmes*, the emails were used against the plaintiff to counter her claim of emotional distress. Employers may encounter similar situations in which internal communications by employees contain information necessary to defend a suit. Hence, employers should take steps so that employees cannot assert a claim of privacy as a means to exclude such information.

Companies must have clear, explicit written policies stating that company technology is not for personal use and that any electronic communication is not private. If an employer already has in place such policies, then it is important that the employer review those policies regularly and update them, if necessary. Technology constantly changes, and an employer's policies must be tailored so that an employee will not believe that some communications may be monitored while other communications may be deemed private.

Most importantly, employers must enforce these policies routinely and consistently. Although the "operational reality" test did not apply in *Holmes*, the Third District suggested that the test may apply under a different set of facts. To avoid this scenario, all employers must maintain a policy that is followed consistently. Employers should have a monitoring system of computer technology in place, and should discipline employees who do not follow the policies. In addition, supervisors must not indicate to employees that the policy is not followed, or represent that an abuse of the policies will go unpunished. A lackadaisical approach to enforcement may lead to mixed messages as to whether an employee's computer use is private. If a company's operational reality is not to enforce the policy, then the "smoking gun" information that you want to use in your defense may not be admissible.

Holmes provides employers an additional safeguard against employees who use company technology for personal use. It warns employees that their personal use of company technology could be used against them in a lawsuit, and that they cannot hide behind a wall of privacy.