Your Workplace Computer Is a Lonely Public Roadway

By Eli M. Kantor
and Zachary M. Cantor

According to the 3rd District Court of Appeal in *Holmes v. Petrovich*, 2011 DJDAR 671, your office privacy is a lonely public roadway. And where the limits are clearly posted, you had better obey — no matter what kind of car you drive.

In *Holmes*, an employee communicated the particulars of a potential sexual harassment claim against her employer to her attorney via e-mail, from her company computer. But company policy — of which Holmes was well aware — provided that: company computers were to be used only for company business; the company could monitor its computers for compliance with this policy and thus could "inspect all files and messages at any time" (though it never had); and employees who used company computers to create or maintain personal information or messages "have no right of privacy with respect to that information or message." The court declined to uphold attorney-client privilege, because Holmes knew third parties could have listened in.

Holmes argued that her e-mails were private, and thus protected by attorney-client privilege. She relied on *City of Ontario v. Quon* (2010) 130 S.Ct. 2619, a recent U.S. Supreme Court decision, to bolster her claim. In *Quon*, the police department reviewed an officer's *text messages; graphic messages* he sent to his girlfriend over a city-issued pager during work hours. Quon argued that the city's actions violated his Fourth Amendment right to be free from "unreasonable searches." Although the police department's usage policy stated that messages might be audited, the established practice was not to audit the messages so long as employees paid overage charges. Quon argued that his superior's oral assurances that the policy was not actually enforced overrode the policy itself. But, while the Court assumed he had a right to privacy, it deemed the department's search reasonable under the Fourth Amendment.

The court in *Holmes* did not find the privacy argument persuasive. Just because the policy was not enforced did not mean that it did not exist — and Holmes' employer had not issued any contradictory statements that could override the policy. The court stated: "Just as it is unreasonable to say a person has a legitimate expectation that he or she can exceed with absolute impunity a posted speed limit on a lonely public roadway simply because the roadway is seldom patrolled, it was unreasonable for Holmes to believe that her personal e-mail sent by company computer was private simply because, to her knowledge, the company had never enforced its computer monitoring policy."

In other words, Big Brother made it clear that he would be watching. He can turn the surveillance camera on at any time. So don't whine that there was no warning.

> In the age of red light cameras and global positioning satellites, we tend to ignore all of these electronic eyes.

Nowadays, we have become so accustomed to surveillance. In the age of red light cameras and global positioning satellites, we tend to ignore all of these electronic eyes. We act as if our tweet, posts, and texts are hidden from public view, even when we are using company-issued electronic devices. But the trend in the law is just the opposite: rather than creating a broad expectation of privacy, the *Holmes* court has seemingly ushered in a new expectation of responsibility.

That is why the onus is wholly on attorneys, employees, and employers to use discretion. We must act as if every tweet, post and text could end up splashed across the front page of the *Times*, or as an exhibit at trial. With newfound clarity from *Holmes*, attorneys should add to the long list of client admonitions the limits of electronic communication on company devices. Attorneys must tell their clients to be clear about company policies. In this regard, employees should become intimately familiar with their employer's privacy and electronic communications policies. And, of course, employers should set firm boundaries for electronic communications in the workplace so that, as in *Holmes*, the employee is put on notice. To be sure, employers should thoroughly explain the policy, require employees to sign off on it, and field any queries an employee might have.

Yet many questions still remain. For example, *Holmes* presents broad implications for the psychotherapist-patient privilege, clergy-penitent privilege, and spousal communications privilege, and how parties engaged in these confidential relationships communicate. Each one of these privileges contains similar, if not identical, language on which the *Holmes* court dwelt in deciding that attorney-client confidentiality had been breached.

Indeed, for a heated argument or steamy flirt to be private under the spousal communications privilege, the communication must have been made in confidence between the spouses. Similarly, feelings expressed to a psychotherapist must be in confidence and, so far as the patient is aware, disclosure of the information to third persons is only permissible to further the consultation's interest. And the clergy-penitent privilege also stands in a similar light. Thus, had Holmes discussed her emotional distress (or lack thereof) with her priest, psychotherapist or spouse, surely the court would have reached the same result.

Moreover, the *Holmes* decision leaves little room for speculation as to which of an employer's electronic devices are safe for private use. And the court did not require Holmes to have composed her personal messages on company time — only on company equipment. Had Holmes used a company-issued Blackberry while at home and off the clock, such distinctions could not have altered the court's reasoning. If Holmes knew that company policy explicitly eliminated her right to privacy regarding all communications made with company equipment, then the time, setting, and device used should make no difference.

Clearly carrying separate devices for work and for play is becoming a necessity. Sure, it's more stuff to carry around. Yes, it costs more money. And yes, you'll look like a geek. But it's probably worth it.

New questions should flicker past your mind's eye during your next commute. If you are an attorney, fresh angst will likely flood your chest when your client sends you an e-mail from a company device. If you are an employee, you will be anxious to find out whether you are being watched. If you are an employer, you will obsess over your company policy. And if you are just about anyone else, you will be concerned with the device from which your spouse, patient, or congregant has communicated to you. But for all concerned, rest assured that "1984" has arrived — albeit in the private sector — and Big Brother is watching.

Eli M. Kantor has extensive experience as an attorney in private practice. He represents employers and employees in all aspects of labor, employment and immigration law. He can be reached at (310) 274-8216 or at ekantor@beverlyhillsemploymentlaw.com.

Zachary M. Cantor, an associate at the Law Offices of Eli Kantor, represents employers and employees in all aspects of labor, employment and immigration law. He also writes and illustrates children's books (zacharycantor.com).