New York Law Journal

Cutting Out Privacy in the Office

Kelly D. Talcott
12-19-2007
For many of us, George Orwell's "1984" was required reading at some point during our formative years. The picture it painted of a world where privacy was virtually nonexistent and the consequences faced by an individual who dared to oppose the system provoked in many of us an almost instinctive reaction against such a totalitarian exercise of raw authority.

In the 23 years since the actual year 1984 came and went -- happily with few of the horrors envisioned by Mr. Orwell when he finished the novel back in 1948 coming to pass -- we have allowed our privacy to seep away. Instead of ceding control of our private information to a single all-powerful regime, however, we dole it out in bits and pieces to a diffuse network of eager information-gatherers, many if not most of them in the private sector.

Sometimes we trade it willingly for the sake of convenience, as when we disclose a credit card number to a voice over the phone or a Web site over the Internet. Sometimes we reveal ourselves without knowing it, as when the Web sites we visit are tracked and recorded by small programs surreptitiously loaded onto our computers, which report our meanderings to some private master, usually an advertising company. Sometimes we may not think about it very much, as when we hand our drivers' license to a guard in the lobby of an office building who asks for our identification and then scans the license into the building's computers.

Our MetroCards can track the subway stations we use; E-ZPass records the tolls we pay; our cell phone records detail the calls, text messages, and pictures we send and receive. Google or Hotmail or Yahoo hold our e-mails for us and, increasingly, our personal documents, images, spreadsheets, financial records and even (in a recent venture) personal medical records. Surveillance cameras have blossomed in such numbers that, at any moment when out in a public or semi-public space, it is not unreasonable to assume that our grainy image is being recorded by someone.

It should thus come as no surprise that communications made during work hours may likewise be less than private, even if they relate to purely personal matters. On reflection, this is not unreasonable; communications systems are to today's offices what the

assembly line was to Henry Ford: They are the instruments by which the employer makes money. It is far from unreasonable for employers to place restrictions on how those systems can be used by employees. And because so much of what happens in business is recorded by those systems, it is just as reasonable to expect employers to be able to monitor the information exchanged over those systems by company employees.

A recent New York case provides a careful analysis of the factors that courts consider when determining whether an employee has a reasonable expectation of privacy in private communications made using a company computer system. *Scott v. Beth Israel Medical Center*[FOOTNOTE 1] involved a dispute between Beth Israel Medical Center and a doctor formerly employed there. At issue were e-mails the doctor had exchanged with his personal attorney over the hospital's system while he was still employed there.

The hospital, in the course of collecting documents for discovery, identified the doctor's e-mails with his attorney as being potentially privileged, did not read them and notified the doctor's attorney of their existence. The hospital also stated its position, namely that any potential privileged attached to the communications had been waived by the doctor when he used the hospital's e-mail system to exchange the e-mail with his counsel. The doctor moved for a protective order.

The hospital had in place an e-mail policy that applied to all employees. In essence, it stated that its communications systems were the hospital's property and were to be used "for business purposes only," and that employees "have no personal privacy right in any material created, received, saved or sent" using those systems. The e-mail policy further reserved "the right to access and disclose such material at any time without prior notice."

The hospital argued that its e-mail policy put the doctor on notice that his personal communications should not be considered private and that, whether or not any person at the hospital had reviewed the doctor's e-mails with his attorney, the doctor had waived any claim of privilege with respect to those e-mails.

The doctor first argued lack of notice of the hospital's policy, which the court rejected because as an administrator, the doctor had constructive notice of the policy (he required new hires to acknowledge in writing that they were aware of the policy) and was likely to have had actual notice as well, since the hospital provided "internet notice" of the policy. The doctor also argued that New York's Civil Practice Law and Rule 4548 invalidated the hospital's policy.

CPLR 4548 states that "no communication ... shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication." The court noted that CPLR 4548 does not preclude an employer from adopting a "no personal use" e-mail policy such as the one in place at the hospital.

FOUR-PART TEST

In denying the doctor's motion for a protective order, the court also turned for guidance to a Southern District of New York bankruptcy case that was "virtually identical" to its case. In this case, *In re Asia Global Crossing, Ltd.,*[FOOTNOTE 2] the bankruptcy court set forth a four-part test to use when determining whether the attorney-client privilege

would apply to personal e-mails exchanged by an employee with an attorney over a company-controlled communications system.

The privilege would not apply where (a) the company maintains a policy that bans personal or other objectionable use; (b) the company monitors employee use of computers or e-mail; (c) third parties other than the employee have a right to access the computer and the employee's e-mail; and (d) the company notifies the employee of its use and monitoring policies.

With this test in hand, the court in *Beth Israel* concluded relatively quickly that there was no privilege that attached to the doctor's e-mails with his attorney made over the hospital's systems. The hospital's policy tracked the four factors set forth in *Asia Global*, and the court found evidence that the doctor had actual or constructive notice of that policy.

This decision serves as an important reminder to employers and employees alike. Both need to appreciate the perhaps unintended consequences of policies that are necessarily in place so employers can repair, maintain and upgrade their vital communications systems, as well as protect themselves against misuse of those systems by employees.

PERSONAL ACCOUNTS

Another case underscores a related point: Employees also need to understand that using a personal e-mail account at work, such as a Gmail or Hotmail account, does not necessarily guarantee that their communications will be kept private.

In an unreported decision,[FOOTNOTE 3] a Southern District of New York magistrate judge found that an employer's computer system created and stored temporary copies of e-mails exchanged by employees and their counsel via the employees' personal, password-accessed e-mail accounts. Because the employees were on notice of the employer's policy (a policy similar to the ones considered in *Beth Israel* and *Asia Global*), the court held that the employees had waived any privilege that may have attached to those e-mails.

These cases do not address the situation where an employer institutes a policy that permits some personal use of firm communications systems, but still retains the right to access all systems and to review all communications. They also do not discuss the implications of the waivers that were found to have occurred. Presumably the employees in these cases had some communications with their attorneys away from the office. Should the waiver of the privilege caused by the employees' use of company computer systems result in a waiver of the privilege as to all other communications with counsel on the same topic as well?

They also do not address the situation of voice mail or phone communications. In many companies, telephone systems are now integrated with company computer systems; indeed, many phone conversations are carried over the Internet via so-called "VoIP" systems and no longer use traditional phone lines, at least within the confines of the employer. In those cases, does the broad language of the company's communications policy allow the company to eavesdrop on the employee's conversations or capture and record them on a company server?

The clearest advice for employees wishing to confer with their personal attorneys during business hours would be to make sure that all remote communications take place over communications devices that are controlled by the employee -- a personal cell phone, home computer and home phone lines.

Employers, on the other hand, may want to weigh the relative merits and problems associated with creating a "limited personal privacy exemption" for employees using company communications systems. While such an exemption may come to be considered a valuable benefit, it would have to be carefully crafted to limit liability to the employer.

Perhaps one way might be to provide a "personal Internet use" link on the company system, or "personal use" phone booths and lines, and making it clear to employees how to go about taking advantage of those benefits. The dangers of accommodating such personal privacy, however, may outweigh the benefits.

Kelly D. Talcott is a partner in the New York office of K&L Gates practicing intellectual property and technology law.

::::FOOTNOTES::::

FN1. *Scott v. Beth Israel Medical Center, Inc.*, 2007 WL 3053351 (N.Y. Sup. Oct. 17, 2007).

FN2. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

FN3. *Long v. Marubeni America Corp.*, 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006).