THE NATIONAL LAW JOURNAL

FEBRUARY 1, 2010

Daily Updates at NLJ.COM

An ALM Publication

Time to review corporate computer policies

Three recent cases should prompt companies to address expectations of privacy and permissible access.

BY NICK AKERMAN

Three recent court decisions make it important for companies to begin the new year with a thorough review of their computer-use policies with a focus on two issues: ensuring that employees have no expectation of privacy in using the company computer systems and delineating the scope of the employee's permissible access to the company computers. This article will discuss these three decisions and their implications for creating effective corporate computer policies that protect the company against the theft of its data.

Two of these recent decisions—*Quon v. Arch Wireless Operating Co. Inc.*, 529 F.3d 892 (9th Cir. 2008), cert. granted, 2009 WL 1146443 (2009), and *Stengart v. Loving Care Agency Inc.*, 408 N.J. Super. 54 (N.J. App. Div. 2009)—affect a company's ability to gather evidence from its own computers. Both cases found company computer policies insufficient to defeat the employee's expectation of privacy in using the company computers for personal reasons. Whether an employee has an expectation of privacy on the company computers can become a critical issue when it is suspected that an employee may have stolen corporate data.

THE PRACTICE

Commentary and advice on developments in the law

In *Quon*, the U.S. Court of Appeals for the 9th Circuit held that a review of text messages on pagers provided to municipal police officers violated the Fourth Amendment as an unreasonable search. Although the city had no express policy "directed to text messaging by use of the pagers," it did have a general "Computer Usage, Internet and E-Mail Policy" applicable to all employees that limited the "use of City-owned computers and all associated equipment, software, programs, networks, Internet, e-mail and other systems operating on these computer" to city business.

The policy warned that "[t]he use of these tools for personal benefit is a significant violation of" city policy, that "[a]ccess to all sites on the Internet is recorded and will be periodically reviewed by the City," that the city "reserves the right to monitor...all network activity, including email and Internet use," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." The policy also warned against using "these systems... for personal or confidential communications" because the information produced on the system "is considered City property." This policy was acknowledged in writing by each city employee, and it was announced orally that this policy applied to pagers.

The 9th Circuit affirmed the district court's finding that Jeff Quon had a reasonable expectation of privacy with respect to the text messages because the policy did not reflect the "operational reality" at the police department where the staff were told that the department "would not audit their pagers so long as they agreed to pay for any overages" that exceeded a "25,000 character limit." Id. Consistent with that informal policy, Quon had exceeded that limit " 'three or four times' and had paid for the overages every time without anyone reviewing the text of the messages," demonstrating that the police department "followed its 'informal policy' and that Quon reasonably relied on it."

In *Stengart*, the issue of the computer policies arose in the context of the attorney-client privilege. Marina Stengart used her

NICK AKERMAN *is a partner in the New York office of Dorsey & Whitney who specializes in the protection of trade secrets and computer data.*

employer's laptop computer to communicate with her attorney about an anticipated lawsuit against her employer "through her personal, web-based, password-protected Yahoo email account." After Stengart filed a discrimination suit, her then-ex-employer found numerous e-mails on the company computer between Stengart and her attorney. The employer's computer policy was nearly identical to the policy addressed in *Quon* with one significant exception. Unlike the written policy in *Quon*, which limited use of the computers to the employer's business, the policy in *Stengart* provided that "[o]ccasional personal use is permitted."

The court found two specific "ambiguities" with the computer policy that "cast doubt over the legitimacy of the company's attempt to seize and retain personal e-mails sent through the company's computer via the employee's personal email account." First, the "policy neither defines nor suggests what is meant by 'the company's media systems and services,' nor do those words alone convey a clear and unambiguous understanding about their scope." Second, the court found that one could reasonably conclude "that not all personal emails are necessarily company property because the policy expressly recognizes that occasional personal use is permitted." Given these ambiguities, Stengart could have assumed her e-mails with her attorney would be confidential.

The third decision relates to a company's ability to use evidence found on its own computers to bring a viable court action against the disloyal employee under the federal Computer Fraud and Abuse Act (CFAA) to retrieve the stolen data and prevent its dissemination in the marketplace. The CFAA, the federal computer crime statute, provides a civil remedy for a company that "suffers damage or loss" by reason of a violation of the CFAA. 18 U.S.C. 1030(g). A critical element in proving most CFAA claims is that the violator accessed the computer "without authorization" or "exceeding authorized access."

THE ISSUE OF PERMISSIBLE ACCESS

That case, *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), has made it more important than ever for corporate computer policies to address what is not permissible access to the company computer system. Until *Brekka*, no other circuit court had disagreed with the 7th Circuit's holding in *Int'l Airport Centers LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), that an employee's authorization to access the company computers is predicated on his agency relationship with his employer such that when an employee violates his duty of loyalty by stealing his employer's data, his authorization to access the company computers terminates. *Brekka* refused to apply the CFAA to a theft of employer data, holding that employees cannot act "without authorization" because their employer gave them "permission to use" the company computer.

Although this division in the circuit courts will ultimately have to be resolved by the U.S. Supreme Court, from an employer's standpoint it is important to emphasize that the agency relationship with the employee is not the only way to prove that an employee's access to the company computer was unauthorized or exceeded authorization. Employers can proactively establish the predicate for unauthorized access by promulgating the rules of access through company policies. The "CFAA…is primarily a statute imposing limits on access and enhancing control by information providers." *EF Cultural Travel B.V. v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003). Thus, a company "can easily spell out explicitly what is forbidden" through a compliance code or an employee handbook or through employee agreements. See *Cont'l Group Inc. v. KW Property Mgmt.*, 622 F. Supp. 2d 1357 (S.D. Fla. 2009); *EF Cultural Travel B.V. v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001).

In designing corporate computer policies and employee agreements, it is important not to lose sight of the well-established operating principle that company computers are company property, and, as such, the company can "attach whatever conditions to their use it wanted to," even if these conditions are not "reasonable." *Muick v. Glenarye Electronics*, 280 F.3d 741, 743 (7th Cir. 2002). Nonetheless, in light of *Quon*, *Stengart* and *Brekka*, a company should review its computer policies to ensure that they do the following:

- Clearly define the computer systems covered by the policy; expressly encompass whatever technology is used, such as text messaging or instant messaging; and address not only the servers but removable media such as thumb drives and disks.
- Make clear that all data created in furtherance of any personal use belongs to the company—including use of the company systems to access personal Web-based e-mail accounts—and may be monitored by the company and will not be confidential.
- Reflect operational reality and are audited at least annually to ensure they reflect operational reality.
- Spell out precisely the scope of an employee's permissible authorization to the company computers, particularly what they are not permitted to do, e.g., access the company computers to retrieve company data for a competitor.

The time to get this right is now before the company finds itself the victim of a data theft. ■