New Jersey Law Journal

VOL. CXCVIII – NO. 10 - INDEX 800 DECEMBER 7, 2009 ESTABLISHED 1878

Employment & Immigration Law

Cyberspace in the Workplace

Employer protection requires a more than mere ownership of the computer systems

By Denise J. Pipersburgh and Keyana C. Laws

Employee e-mail use in the workplace is a hot topic these days. Certainly, employers are concerned with curtailing employee abuse of company e-mail systems during working hours and guarding against the unauthorized dissemination of confidential business information or trade secrets. As a result, many employers have implemented e-mail and Internet use policies which not only assert that information stored in the employer's computer systems belong to the employer, but also reserve the employer's right to access and review e-mail communications and other information stored on its systems. Many employers have taken the stance that such broad policies give them the right to access an employee's personal, password-protected, Web-based e-mail account where the employee's username and password have been stored in the employer's computer. However, as more courts around the nation weigh in on this issue, there is increasing evidence that an employer's right to access an employee's personal e-mails has distinct boundaries.

One of the key decisions in this debate has recently come from the New Jersey Appellate Division. In *Stengart v. Loving Care Agency, Inc*., 408 N.J. Super. 54 (App. Div. 2009), the plaintiff, a former employee of Loving Care, was provided a company-owned laptop computer, which was returned to Loving Care when she resigned. Shortly thereafter, Stengart filed suit against Loving Care alleging, among other things, violations of antidiscrimination laws. In preparation to defend the lawsuit, Loving Care reviewed the contents of the laptop's hard drive and discovered e-mails between Stengart and her attorneys. As the litigation developed, these e-mails were identified and referenced by Loving Care in its discovery responses. Stengart applied for an order to show cause with temporary restraints to prohibit Loving Care from using and referencing such e-mails. The trial court denied the plaintiff's motion, finding that the employer's policy put Stengart on notice that such e-mails would be viewed as company property.

However, the New Jersey higher court reversed the trial court's denial of the plaintiff's motion. The Appellate Division determined that the employer's policies did not give it the right to access e-mails shared between Stengart and her attorneys because Loving Care had no legitimate business interest in accessing Stengart's personal e-mails. Unlike the trial court, the Appellate Division gave little credence to the employer's policy, which explicitly stated that it had the right to review and access all information in its computer systems. Rather, the court held Loving Care to a higher standard than previously expressed under New Jersey law. The Appellate Division required that, in order to assert its right to access such information, Loving Care must articulate a more plausible rationale than mere ownership of the computer systems.

New Jersey is hardly the first jurisdiction to examine this dilemma, and this state's resolution of the issue does not stand alone. In *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008), the employee-defendants were sued by their former employer, Pure Power, for breach of their noncompete agreements. Upon resigning from Pure Power, the employees, Alexander Fell and Ruben Belliard, opened up a competing fitness center. After the employees' resignation, the company accessed and reviewed e-mails from three of Fell's personal e-mail accounts using, among other tactics, his login information stored on its computers. Fell's personal e-mails illustrated his efforts to establish the competing fitness center, and were compelling evidence to

Pipersburgh and Laws are associates with Wolff & Samson in West Orange.

support Pure Power's allegations against the employees for violation of the noncompete agreements. However, the Southern District Court of New York precluded Pure Power from using these personal e-mails as evidence, despite the company's policy that purportedly covered e-mails sent or received from personal e-mail accounts accessed through the employer's system.

Up until now, it has been presumed that a robust Internet and e-mail policy would absolve an employer of potential liability under the Stored Communications Act (the "SCA"), because such a policy would provide the employer with the requisite authority under federal law to permissibly access an employee's e-mails where the login information is stored on its computer system. Under the SCA, anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and by doing so "obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system" faces criminal and civil liability. 18 U.S.C.A. Section 2701 et. seq. However, consent provides an exception to liability under the SCA. As such, there is no violation for accessing another's electronic communications where either the sender or recipient gives his or her consent to permit another to access such information.

The *Pure Power* decision relied, in part, on the SCA as support for its findings. There, the employer's policies permitted Pure Power to review its employees' personal e-mail accounts that were accessed via its computer system. However, the district court determined that since such e-mails were not stored in Pure Power's systems but with outside providers and were not necessarily created or sent from the employer's computers, the policy was inapplicable. The district court rejected the employer's presumed authority by emphasizing that the e-mails were not stored in the employer's computer system, but merely accessed from it on a single isolated occasion. According to the district court, the fact that the login information was stored on the employer's computer systems did not actually mean that the employer could use it to access the accounts without the employee's consent where the contents of the e-mail accounts were stored with an outside provider. Further, consent could not be obtained from the employee through Pure Power's policy, as the policy neither asserted nor suggested that the employer's authorization to review personal e-mails extended beyond its own computer system.

In contrast, the *Stengart* holding does not discuss, nor is it based upon, the SCA. Rather, the New Jersey Appellate Division directly challenged the notion that a workplace policy could, by itself, convert an employee's personal e-mails into company property. The *Stengart* Court defeated the presumption that an Internet and e-mail policy, however broad, could provide an employer with the authority to access an employee's personal e-mails. Further, the *Stengart* holding calls into question any policy that purportedly gives an employer the authority to access an employee's personal e-mails without greater justification than mere ownership of the computer system. The New Jersey Appellate Division concluded that, in order for the employer's policies to be given full effect, such policies must be reasonable in nature and must concern the legitimate business interests of the employer.

In deciding not to import the SCA into its analysis, the New Jersey Appellate Division significantly broadened an employee's right to privacy in the workplace. Despite the Appellate Division's assertion that its holding may not be applicable in all circumstances, its conclusion indicates the opposite. If this holding is to be given full effect, the implications for all employers are overwhelming: where e-mail accounts are clearly personal and do not pertain to the employer's business or reputation, an employer's policies cannot assert ownership and control over their contents. This raises the necessary inquiry of whether this holding could be extended to all personal e-mails sent and received through an employer's systems. While an employer's legitimate business interests in its own computer system are readily discernible, if the employee's personal e-mails do not pertain to the employer's business or reputation, it may be asserted that, as with call monitoring policies, the employer is prohibited from reviewing the contents of the e-mail. Notably, *Stengart* does not prohibit an employer from monitoring an employee's use of personal e-mail accounts. The decision does, however, restrict the employer from accessing, monitoring or confiscating the contents of the e-mail accounts and the e-mails themselves.

When *Stengart* is analyzed in conjunction with *Pure Power*, the landscape of employee privacy rights in the workplace becomes substantially broader than previously believed. Even if the e-mails relate or impact the employer's business and/or reputation and fall within the narrow exception delineated by the New Jersey Appellate Division, an employer may still be precluded from accessing such e-mails under similar circumstances when the login information to access such personal e-mail accounts, and not the e-mails themselves, are stored in the employer's systems. Taken together, these cases significantly limit an employer's control and access over an employee's personal e-mail accounts and e-mails, even where an employee may be disseminating the employer's confidential trade secrets or blatantly violating company policy in his or her use of the Internet in the workplace.

The New Jersey Supreme Court recently granted Loving Care's appeal of the Appellate Division's decision, which raises the question of whether this expansive holding will withstand further scrutiny or contract an employee's right to privacy in the workplace. As New Jersey courts, and other courts around the nation, sort through the questions left unanswered by the growing number of cases addressing these issues, it remains to be seen how great the strength of employee privacy claims in the workplace may become in this new digital age. ■