

JANUARY, 2006

1300 MOUNT KEMBLE AVENUE
P.O. BOX 2075
MORRISTOWN, NJ 07962-2075

TELEPHONE (973) 993-8100
FACSIMILE (973) 425-0161
www.mdmc-law.com

Employment Bulletin

EMPLOYER FACES LIABILITY TO THIRD-PARTY FOR FAILURE TO MONITOR EMPLOYEE'S COMPUTER ACTIVITY

McElroy, Deutsch, Mulvaney & Carpenter, LLP 2006 Decision Review, No. 1
John T. Coyne, Esq.

From a face-on view, it is virtually impossible to tell whether an employee at a computer workstation is diligently discharging his job duties, participating in purely social e-mail discourse, checking the previous day's sports results or engaging in far more pernicious activity. Tracking an employee's computer usage, of course, requires more than casual observation and entails expenditure of manpower and money. Is it, therefore, permissible for an employer to dispense with the effort and elect to not monitor computer activities? Not necessarily, per the recent decision in Jane Doe v. XYZ Corporation, 2005 N.J. Super. LEXIS 377 (App. Div. Dec. 27, 2005). Presented with some unusual facts, the court held that an employer was bound to investigate and, if necessary, prevent one of its 250 employees from trafficking in child pornography. The court proclaimed that "[n]o privacy interest of the employee stands in the way of this duty on the part of the employer." For failing to take appropriate remedial measures, the employer opened itself to liability to a third-party victim of what the court described as a societal "scourge."

As is customary, the employer had promulgated a policy prohibiting non-business use of office computers. The employer, however, also had implemented a rule against monitoring computer activity. The odd combination of policies appeared to reflect a decision by the employer to not actively enforce the computer-for-business policy and instead to rely on its mere promulgation as having some deterrent effect. The employer serendipitously discovered that an employee had been visiting pornographic websites (apparently through a systems administrator's violation of the no-monitoring policy.) The employer reprimanded the employee and directed that he cease the improper activity. For a short period, the employee refrained from visitation of inappropriate websites, but then resumed his illicit behavior and transmitted three pornographic images of the minor plaintiff from his computer workstation.

The employee's acts obviously fell outside the scope of his employment. The court, however, invoked the Restatement (Second) of Torts, Section 317 (1965) which provides:

A master is under a duty to exercise reasonable care so to control his servant while acting outside the scope of his employment as to prevent him from intentionally harming others or from so conducting himself as to create an unreasonable risk of bodily harm to them, if

- (a) the servant
 - (i) is upon the premises in possession of the master or upon which the servant is privileged to enter only as his servant, or
 - (ii) is using a chattel of the master, and
- (b) the master
 - (i) knows or has the reason to know that he has the ability to control his servant, and
 - (ii) knows or should know of the necessity and opportunity for exercising such control.

Subsection (a) is disjunctive and in cases involving employer-owned desktop or laptop computers, prong (ii) necessarily will be satisfied. The key, therefore, will be the subsection (b) inquiry.

The employer argued that Blakey v. Continental Airlines, Inc., 164 N.J. 38, 61(2000) absolved it of liability. In Blakey, the New Jersey Supreme Court emphatically declared that employers have no duty to monitor employees' e-mail, adding that monitoring would implicate "grave privacy concerns." Courts in many other States have held that employees can harbor no reasonable expectation that their business computer use will remain private. As a tribunal of inferior jurisdiction, however, the Doe court was not able to adopt that line of authority. Instead, the Doe court appeared to limit Blakey to "private communications" (i.e., e-mail) and declined to extend it to websurfing.

The e-mail versus websurfing distinction is a rather slender reed and does not appear to provide an adequate foundation for a decision as significant as Doe. Perhaps a better basis for reconciling Doe and Blakey is the nature of inquiry-triggering information. In Doe, the employer possessed antecedent actual knowledge of the employee's appetite for internet pornography (though the employer was arguably unaware that the employee frequented child pornography sites.) Doe held that, in the face of such knowledge, the employer is bound to take some action. Absent such particularized knowledge, however, Doe does not impose on employers any prophylactic duty to monitor and, thus, does not conflict with the Blakey holding. (The employer already had monitoring software in place. The Doe court, therefore, engaged in no discussion regarding the burdensomeness or cost of the monitoring.)

Plaintiff attempted to hold the employer liable for a wide range of damages, arguing that, if the employer had conducted a prompt and proper investigation and made a corresponding report to law enforcement authorities, the employee would have been incarcerated, terminating the predatory pornographic activity inside and outside the workplace. The court sidestepped the scope of damages issue, finding that plaintiff had waived all claims except those stemming directly from the dissemination of her images from the workplace computer. If the court had addressed the issue on the merits, it appears that Section 317 would have dictated the same result. The touchstone of Section 317 liability is control and the employer controls only the use of its computer, not all external activities of employees.

Child pornography is perhaps the most depraved and antisocial behavior known to civilized society. From the Doe court's framing of the issue as a balance between eradication of child pornography and preservation of an amorphous privacy interest in workplace computer activity, it is easy to predict the result. Indeed, if the judicial motivation was to create incentives to ferret out those who feed the industry, it is difficult to quarrel with that objective. The key question is whether Doe will be confined to its facts or whether the monitoring obligation will be extended to other circumstances. What if an employee is suspected of visiting websites with instructions for making bombs, printing counterfeit lottery tickets or profiting from insurance fraud? Will employers face liability to third-party victims? Claimants in search of deep pockets undoubtedly will seek liberal imposition of the Doe duty. Each case will present its own factual and legal variables and case-by-case analysis will be necessary. Until the contours of the monitoring duty are more clearly-defined, all employers should be aware that a door to potentially-expansive liability has been opened.

765229