



October 23, 2007 by: Dino Tsibouris & Mehmet Munur



Dino Tsibouris  
(614) 360-1160  
[www.tsibouris.com](http://www.tsibouris.com)  
[dino@tsibouris.com](mailto:dino@tsibouris.com)

## E-COMMERCE AND HUMAN RESOURCES

This issue will examine a case limiting an employer's ability to supervise an employee's private email and another case approving ESIGN use in electronic job applications.

### **HR policy did not allow employer to read copies of employee's Yahoo email recovered from company laptop.**

If an employer wishes to read an employee's attorney-client privileged communications both made via a private, password protected email account and stored in the temporary files of a company-owned laptop, then the employer must plainly communicate this wish, ruled a Massachusetts court.

David Evans entered into a non-solicitation agreement with his employer. Before Evans left for a competitor, he consulted his attorney using his password protected Yahoo account on his company laptop. Unknown to Evans, all information Evans accessed on the internet was recoverable by his employer from the laptop's hard-drive in a "screen shot" form. These shots were inaccessible to an average computer user. However, his employer used a forensic expert to recover the emails after he left and wanted to use them in litigation.

The employer claimed his emails to his attorney were not privileged because the HR manual stated that 1) employee emails were not confidential and 2) all internet activity was logged, including sites and emails. Therefore, Evans' email communications over Yahoo could not have been in confidence.

The court disagreed because 1) the manual was not directly on point and 2) Evans' actions were adequate under the circumstances to secure confidentiality. First, the court conceded that employer email accounts would not have been confidential due to the manual. However, Evans' Yahoo email was different. NERA's manual only stated that the websites visited would be logged, not their *content*. Second, Evans

had never attempted to store the emails in his NERA email account, or in any other document on the hard-drive. Before turning over his laptop, Evans had deleted all of his personal files but left intact all work related files. Evans even defragmented the laptop's hard-drive—hoping it would prevent the recovery of the deleted files. Therefore, the court ruled that Evans' emails were protected under the attorney-client privilege.

The opinion is significant because the court fell just short of ruling an employer cannot breach a certain level of privacy—no matter the employee handbook. The court recognized the extreme difficulty a travelling employee would face to secure confidential communications with his attorney, which could only be solved by the employee carrying two laptops—one personally owned, the other employer owned.

In addition, employers wishing to read private emails may face tougher challenges due to changing technology. Email service providers have started offering encrypted email access, which displays a prominent padlock icon on the browser address bar. This icon may lead employees to reasonably, but falsely, believe that their communications are secure from their employers. Therefore, an employer may not be able to read employees' private emails without an explicit announcement about the recoverability of private communications.

The case is *National Economic Research Associates, Inc. v. David Evans*, 2006 Mass. Super. LEXIS 371 (Mass. Super. Ct., Aug. 3, 2006).

### **Court Upholds Use of ESIGN Act to Apply Online at Kiosk.**

When an employee agrees to the terms of an electronic agreement through two affirmative clicks, an employee is bound by the terms of that agreement, an Ohio court held.

Lasunda Bell applied for employment at Hollywood Entertainment using an electronic kiosk, which included two questions that specifically referred to an arbitration program. First, the kiosk asked Bell whether she knew

how to access the arbitration rules online. Second, the kiosk asked whether Bell agreed to arbitrate all claims related to her employment. Bell clicked in the affirmative to both questions. Arguing that an electronic signature is binding under the Electronic Signature in Global and National Commerce Act (ESIGN), the court upheld the arbitration provision referenced at the kiosk.

Curiously, the court did not analyze whether the arbitration clause was properly incorporated into the employment agreement. One of the kiosk questions included a hyperlink to the arbitration rules, but neither asked Bell whether she had read them. Moreover, Bell was not able to visit the website with the arbitration rules using the kiosk.

Recently, both courts in *Affinity Internet Inc., v. Consolidated Credit Counseling Services*, 920 So. 2d 1286, 1287 (Fla. Ct. App. 2006), and *Manasher v. NECC Telecom*, No. 06-cv-10749 (E.D. Mich. Sept. 18, 2007), held that a mere reference to a hyperlink containing additional clauses did not properly incorporate those term into a contract. Therefore, those additional terms were unenforceable. Similarly, Hollywood did not properly incorporate the arbitration clause into Bell's employment agreement.

Admittedly, Bell agreed to arbitrate her claims with Hollywood by clicking in the affirmative to the second arbitration question at the kiosk. As a result, Bell's arbitration would be governed by that question, not by the document that Hollywood Entertainment referenced in the hyperlink. While practically this makes little difference, another court could

have been more critical.

In sum, neither electronic kiosks nor online applications will be struck down by courts solely due to their electronic nature. Furthermore, employers should properly incorporate virtual documents into actual agreements.

The case is *Bell v. Hollywood Entm't Corp.*, 2006 Ohio 3974, P3 (Ohio Ct. App. 2006).

+++++

Mr. Tsibouris helps corporate clients comply with privacy law, license technology and deliver electronic financial services.

You may reach him at (614) 360-1160 or [dino@tsibouris.com](mailto:dino@tsibouris.com).

This Privacy and Security Update is intended to provide information about important legal developments, not legal advice. Readers should consult legal counsel for advice about their specific circumstances.