Snell & Wilmer L.L.P.

THE WORKPLACE WORD

www.swlaw.com February 2008

EMPLOYER IMMUNITY FOR EMPLOYEE CYBERTHREATS?

MAY AN EMPLOYER BE HELD LIABLE WHEN ITS EMPLOYEE USES THE EMPLOYER'S INTERNAL COMPUTER SYSTEM TO COMMUNICATE THREATENING MESSAGES?

The federal Communications Decency Act of 1996 ("CDA"), 47 U.S.C.S. §230, generally affords **immunity** to a cause of action that would make a computer service provider liable for information originating with a third-party user. However, the question as to whether this immunity extends to employers who provide internet and e-mail access to its employees was unclear.

In *Delfino v. Agilent Technologies, Inc*., the California Court of Appeals addressed this very issue. The Plaintiffs had received several anonymous threats that were sent via email or posted on a Yahoo! Message Board. Plaintiffs contacted the FBI and the FBI was ultimately able to trace the messages and postings to an employee of Defendant Agilent Technologies, Inc. ("Agilent"). Agilent and the FBI investigated the matter, which led to the arrest of the employee, as well as the discovery that the employee had made the threats using Agilent's internet and email systems. One week after the employee's admission, Agilent terminated the employee's employment.

Plaintiffs sued Agilent and the employee for intentional and negligent infliction of emotional distress. They alleged that Agilent was liable for the employee's threatening messages: (1) because it ratified his actions; (2) under the theory of *respondeat superior*; and (3) because it was negligent in its supervision and retention of the employee. Plaintiffs further claimed that Agilent was aware the employee was using its computer systems to send and post the threats, and yet took no action to prevent the employee from doing so.

Agilent argued that it was immune from liability under Section 230 of the CDA, which states in part: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). The California

contacts

DENVER
Katrin Rothgery
303.634.2047
krothgery@swlaw.com

LAS VEGAS
Swen Prior
702.784.5262
sprior@swlaw.com

ORANGE COUNTY
Christy Joseph
714.427.7028
cjoseph@swlaw.com

PHOENIX
Manuel Cairo
602.382.6534
mcairo@swlaw.com

SALT LAKE CITY
David Williams
801.257.1914
dawilliams@swlaw.com

TUCSON
John A. Robertson
520.882.1206
jrobertson@swlaw.com

Court of Appeals agreed, confirming that Agilent was an "interactive computer service provider" immune under the CDA from liability for alleged damages arising from its employee's cyberthreats. In coming to this conclusion, the court analyzed whether Agilent satisfied the three essential elements to qualify for CDA immunity: (1) the defendant is a provider or user of an interactive computer service; (2) the cause of action treats the defendant as a publisher or speaker of information; and (3) the information at issue is provided by another information content provider.

Even if Agilent was not entitled to CDA immunity, the court explained that Plaintiffs still failed to establish their case for intentional infliction of emotional distress or negligence. It reasoned that Agilent investigated the threats, terminated the wrongdoing employee's employment, and did not ratify the employee's conduct. Furthermore, the employee's conduct was personal and not within the scope of his employment.

What Employers Need To Know

The *Delfino* case confirms that employers who provide their employees with internet and e-mail access may be protected under the CDA against suits for damages arising from an employee's misuse of that access.

Employers can and should, however, take action to minimize their liability. Employers should be vigilant in their efforts to ensure that their employees are properly using their electronic systems. Employers may also consider the following measures:

1. Develop, distribute, and enforce a policy regarding the use of electronic equipment. This policy must set clear guidelines for the appropriate use of the internet, e-mail, blogging (both using company assets and with respect to blogging about the company using personal assets), voicemail, and any company intranet or electronic bulletin boards. It is also important that the policy be protective of the company, yet practical in recognition of the extensive role technology plays in the lives of employees.

2. Quickly act on reports of suspected misuse of the company's electronic assets. The employer should conduct a prompt and thorough investigation. When necessary, the employer should take disciplinary action – up to and including termination, and/or taking other remedial measures to prevent any future misuse.

If you have any questions about this topic or any other Workplace Word, please feel free to contact us.

* * *