

Are Employers at Risk When Employees Use Office Computers to Send Cyber-Threats or Post Offensive Materials On-Line?

When a rogue employee uses an office computer to send or post threats of great bodily harm, or is the source of other highly offensive information, an employer sued for such activity can assert the immunity defense under the Communications Decency Act of 1996 (CDA), 47 U.S.C. § 230. This federal law defense preempts inconsistent state law that might otherwise impose liability and immunizes “provider[s] . . . of an interactive computer service” (the employer) where “another information content provider” (the employee) has initiated the offending activity. While the facts considered recently by a California Court of Appeal in *Delfino v. Agilent Technologies, Inc.* (2006) 145 Cal.App.4th 790 are unquestionably extreme and will not likely be encountered in garden-variety employment situations, the CDA immunity defense could well apply in more benign or commonplace circumstances.

Here’s the scenario considered in *Delfino*: Unbeknownst to his employer, an angry employee sends anonymous emails to his adversaries, and creates posts on Internet bulletin boards, threatening great bodily harm and death. The employee uses the computer systems of his employer. The victims of these scary threats contact the FBI, who trace the emails and postings to the employee’s office computer, by tracking them back through the originating IP address. The employee admits engaging in the offensive conduct, and criminal charges are filed against him. The employer terminates the offending employee. Seeking recompense, the victims of the employee’s threats sue the employee and the employer for intentional and negligent infliction of emotional distress, and negligent supervision or retention. Plaintiffs claim the employer was aware that the employee was using its computer system to threaten them and that it took no action to prevent its employee from continuing to make his threats over the Internet.

Can the employer be liable under these circumstances? While this scenario may seem far-fetched, it was presented as an issue of first impression in *Delfino v. Agilent*, where a California appellate court determined that an employer could assert the immunity defense under the Communications Decency Act of 1996 (CDA), 47 U.S.C. § 230. Asking the court to toss out the plaintiffs’ case, the employer filed a motion for summary judgment, asserting that it was a “provider . . . of an interactive computer service”, and therefore entitled to complete immunity under the CDA. Section 230(c)(1) states that “[n]o 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.” The statute also preempts inconsistent state law that would impose liability, saying: “Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” Section 230(e)(3), italics added.

While the primary goal of the CDA was to control the exposure of minors to indecent material over the Internet, one of its important purposes “was to encourage [Internet] service providers to self-regulate the dissemination of offensive materials over their services.” *Zeran v. America Online, Inc.* (4th Cir. 1997) 129 F.3d 327, 331, cert. den. (1998) 524 U.S. 937. The CDA also sought to avoid the chilling effect on Internet free speech that would occur if tort liability were imposed upon companies that do not create potentially harmful messages but are simply

intermediaries for their delivery. *Id.* at 330-331. Accordingly, Section 230(c)(2) immunizes from liability an interactive computer service provider or user who makes good faith efforts to restrict access to material deemed objectionable.

Drawing on prior CDA cases outside of the employment context, the Delfino court concluded that there are three essential elements that a defendant must establish in order to claim section 230 immunity: (a) the defendant is a provider or user of an interactive computer service; (b) the cause of action treats the defendant as a publisher or speaker of information; and (c) the information at issue is provided by another information content provider. *Gentry v. eBay, Inc.* (2002) 99 Cal.App.4th 816, 830.

On the first element (whether the employer was a provider or user of an interactive computer service), the court found the question a matter of first impression, saying: “We are aware of no case that has held that a corporate employer is a provider of interactive computer services under circumstances such as those presented here. But several commentators have opined that an employer that provides its employees with Internet access through the company’s internal computer system is among the class of parties potentially immune under the CDA.” *Delfino*, 145 Cal.App.4th at 805. Because courts had previously interpreted the term “interactive computer service” broadly (e.g., *Batzel v. Smith* (9th Cir. 2003) 333 F.3d 1018, 1030, fn. 15, cert. den. (2004) 541 U.S. 1085), the court concluded that the employer was a “provider of interactive computer services” under the CDA. *Id.* at 806.

On the second element (whether the cause of action treated the defendant as a publisher or speaker of information), the court found that plaintiffs, in alleging that the employer was liable for the employee’s cyberthreats, sought to treat the employer “as a publisher or speaker” of those messages. (§ 230(c)(1).) *Id.*

On the third and final element (whether the information at issue was provided by another information content provider), there was no dispute that the employee was the party who had authored the offensive e-mails and postings, and there was no evidence that the employer played any role whatsoever in “the creation or development” of the messages. *Id.* at 807-08.

Thus, the employer had satisfied all three elements in order to establish immunity under the CDA. Accordingly, the court of appeal affirmed the trial court’s grant of summary judgment in favor of the employer, agreeing that the grant of immunity under the CDA was proper. The court also noted that, even if plaintiffs’ claims had not been barred under section 230(c)(1), granting summary judgment to the employer was nonetheless proper, because plaintiffs had failed to establish a prima facie case on their claims against the employer. *Id.* at 808. Specifically, the court concluded that there was no indication that the employer had ratified the employee’s conduct, and that the employer could not be liable under respondeat superior principles. *Id.* at 810-12. Nor was there any basis upon which plaintiffs could assert liability based on negligent supervision or retention principles, since there was no evidence or indication that the employer “knew or should have known that hiring the employee created a particular risk or hazard and that particular harm materialize[d].” *Id.* at 815.

While the court affirmed the longstanding principle that an employer will not be held vicariously liable for an employee's malicious or tortious conduct where the employee substantially deviates

from his employment duties for personal purposes, the court also offered an important teaching point on the concept of ratification under California law. Noting that imposing derivative liability on the employer for an employee's actions need not be founded on respondeat superior, but may be based on the doctrine of ratification (*Murillo v. Rite Stuff Foods, Inc.* (1998) 65 Cal.App.4th 833, 852), the court observed that an employee's actions may be ratified after the fact by the employer's voluntary election to adopt the employee's conduct by, in essence, treating the conduct as it own. *Id.* at 810. What evidence would support the ratification theory? Citing California Civil Code § 2339, the *Delfino* court determined that an employer's failure to discharge an employee after knowledge of his or her wrongful acts may be evidence supporting ratification of an employee's conduct. *Id.*

Lessons learned from *Delfino*? While employers can take comfort that the CDA can offer them immunity if rogue employees make offensive or threatening Internet postings, conservative employers should take corrective actions against offending employees when such conduct is discovered, potentially including termination, if the circumstances so warrant. Employers should also institute policies and procedures that prohibit employees from using the employer's computers to post or send threatening or offensive information. Additionally, since CDA immunity will be lost if the employer cannot establish that the information at issue was "provided by another information content provider", cautious employers will also need to avoid any conduct that would suggest the employer has promoted, sponsored, initiated, or ratified the offending material. For example, if the employee in *Delfino* had been a managerial or executive employee, the outcome may have been different.

For more information, contact Ross Hyslop at rhyslop@mckennalong.com