EMPLOYMENT LAW

Employer Not Liable For Employee's Cyberthreats

By
Raul Cadena, Column Editor

Raul Cadena is a partner at Cadena Churchill, LLP, where he represents plaintiffs in the areas of employment law, including wage and hour class actions, insurance bad faith and personal injury. Mr. Cadena received his Bachelor of Arts from Harvard University and his Juris Doctor from the University of California at Berkeley School of Law, Boalt Hall. Mr. Cadena also studied at the Universidad Complutense in Madrid, Spain. He is a member of the Board of Directors of CASD and has been the Employment Law Column Editor for ***Trial Bar News*** *since 2006. He may contacted by email at:* ***rcadena@ccattorneys.com****.*

Recently, in *Delfino v. Agilent Technologies, Inc.*, 2006 WL 3635399, the Sixth Appellate District found an employer immune from liability for threatening emails communicated via the employer's internet system. By characterizing the employer as an "interactive computer service provider", the appellate court extended the immunity available to providers of interactive computer service under Title 47 of the United States Code §230, also known as the Communications Decency Act of 1996 ("the Act").

Facts

Plaintiffs Michelangelo Delfino and Mary Day alleged that Agilent Technologies, Inc. employee Cameron Moore sent several threatening anonymous emails over the internet using Agilent's computer system. Most of the threatening emails were sent under the screen name "crack_smoking_jesus." One of the emails specifically threatened that its "coming [expletive], and you won't see it. I seriously hope you have health insurance because you're going to get your ass stomped by me and some friends. The best part will be you won't be able to prove it was me...."

The FBI contacted Agilent and explained that plaintiffs were involved in a lawsuit with their former employer, Varian, and had posted tens of thousands of inflammatory messages about Varian executives. The FBI explained that when plaintiffs learned Moore made Internet postings siding with Varian, plaintiffs made a series of Internet postings about Moore.

The FBI further explained that plaintiffs received potentially threatening emails that appeared to come from Moore. Agilent agreed to cooperate fully with the FBI investigation and traced one of the originating IP addresses to the computer assigned to Moore. Agilent met with Moore to obtain his side of the story and to administer "a stern warning." Moore apologized for involving Agilent but denied sending any threatening emails using the Agilent computer system.

Agilent did not have proof that Moore had sent the emails. However, Agilent told Moore that he should not be using Agilent's computer systems for anything related to plaintiffs.

After learning that the FBI planned to arrest Moore, Agilent once again met with Moore. At that time, Moore admitted for the first time that he had sent things that "weren't nice and could be interpreted as threats." Agilent placed Moore on administrative leave and subsequently fired him on the ground that he violated Agilent's Standards of Business Conduct, "specifically misuse of Agilent's assets."

Plaintiffs claimed that Agilent knew about Moore's use of the computer system to send the emails and took no action to prevent its employee from making the cyberthreats. Plaintiffs filed suit and alleged causes of action for intentional infliction of emotional distress and negligent infliction of emotional distress.

The trial court granted Agilent's summary judgment on the ground that "Agilent established that it is immune from liability" under Title 47 of the United States Code §230, also known as the Communications Decency Act of 1996 ("the Act"), because it was an interactive computer service provider. Plaintiffs appealed.

Appellate Court's Analysis

The court noted that the Act's primary goal was to control the exposure of minors to indecent material over the Internet by encouraging Internet service providers to self-regulate the dissemination of offensive materials. The court further noted that the second goal was to avoid the chilling effect upon Internet speech by imposing tort liability on companies that are simply intermediaries for the delivery of messages which are potentially harmful.

As the court observed, the three elements required to claim immunity under the Act are "(1) the defendant [is] a provider or user of an interactive computer service; (2) the cause of action treat[s] the defendant as a publisher or speaker of information; and (3) the information at issue [is] provided by another information content provider." *Gentry v. eBay, Inc.* (2002, 4th Dist. Div. One) 99 Cal. App. 4th 816, 830.

With regard to the first element, the court noted that no case had held that a corporate employer is a provider of interactive computer services and that most cases addressing immunity under the Act involved defamation claims. Nevertheless, applying the most expansive application of the Act, the Court held that Agilent met the definition of the term "provider or user of an interactive computer service" in that it provided or enabled computer access by multiple users because Agilent's proxy servers were the primary means by which thousands of its employees in the United States accessed the Internet.

Next, the court examined the second element and noted that Plaintiffs, in claiming Agilent was liable for his cyberthreats, sought to treat Agilent as a "publisher or speaker" of those messages. Accordingly, the court held that the claims against Agilent treated it "as a publisher or speaker" of Moore's messages and that Plaintiffs' claims were "among those to which immunity under the [Act] potentially applies."

In analyzing the third element, the appellate court noted that Moore was the party who authored the offensive emails and postings; that the allegations of the complaint did not suggest otherwise; and that there was no evidence that Agilent played any role whatsoever in the "creation or development

"of the messages. The court held that Agilent satisfied the third element.

Finally, the court found that plaintiffs had not provided sufficient evidence to establish that Agilent should be held liable under ratification, respondeat superior, negligent supervision/retention or negligent infliction of emotional distress. Accordingly, the appellate court concluded that the trial court correctly granted summary judgment.

CONCLUSION

Unfortunately, the *Delfino* court's broad reading of the Communications Decency Act of 1996 may have unintended consequences in the workplace. For instance, employers may now be tempted to argue that as "interactive computer service providers" they are not required to scrutinize the use of the workplace internet system, including emails that may be construed as harassing or threatening, because such regulation would have a chilling effect on free speech. The *Delfino* decision may provide such employers with immunity for claims arising from such emails. It is unlikely, however, that employers who are made aware that employees are sending harassing or threatening emails to persons outside of the workplace, and who provide little or no guidance to their employees regarding the proper use of the company internet system and fail to take corrective action will be granted immunity under the Act.