Filed 12/14/06

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

MICHELANGELO DELFINO et al., Plaintiffs and Appellants, v. AGILENT TECHNOLOGIES, INC., Defendant and Respondent.	H028993 (Santa Clara County Super.Ct.No. 1-03-CV-001573)

A series of anonymous messages were sent over the Internet that constituted threats to Michelangelo Delfino and Mary E. Day (collectively, plaintiffs). The messages consisted of electronic mail messages (e-mails) sent to Delfino and messages that were posted on Internet bulletin boards. These e-mails and postings were ultimately traced to Cameron Moore. Plaintiffs brought suit against Moore and his former employer, Agilent Technologies, Inc. (Agilent). Agilent moved for summary judgment on various grounds, and the trial court granted the motion on the basis that Agilent was immune from suit under the Communications Decency Act of 1996 (CDA). Specifically, the court held that under title 47 of the United States Code section 230(c)(1),[1] Agilent was a "provider . . . of an interactive computer service" entitled to immunity under the CDA.

Plaintiffs contend on appeal that summary judgment should not have been granted because Agilent was not immune from suit under the CDA. They argue that they made a

[1] Hereinafter, all undesignated statutory references are to title 47 of the United States Code.

prima facie showing of negligence. We conclude after a de novo review that Agilent was an interactive computer service provider; as such, it was immune from liability for alleged damages arising out of the cyberthreats transmitted by its employee, Moore. We hold further that plaintiffs did not make a prima facie showing to support a claim against Agilent under theories of ratification, respondeat superior, or negligent supervision/retention. We therefore find that summary judgment in favor of Agilent was proper and will affirm.

PROCEDURAL HISTORY[2]

The complaint was filed on July 22, 2003.[3] It included a claim for intentional infliction of emotional distress and a purported claim for negligent infliction of emotional distress against Moore and Agilent.[4] Plaintiffs claimed that Moore sent a number of anonymous threats over the Internet and that he used Agilent's computer system to send these threats. Plaintiffs alleged further that Agilent was aware that Moore was using its computer system to threaten plaintiffs and that it took no action to prevent its employee from continuing to make his threats over the Internet.

---

[2] To avoid repetition, we present in detail the substance of Agilent's motion for summary judgment and plaintiffs' opposition thereto in part III, sections A and B, of the Discussion, *post*.

[3] Plaintiffs have represented themselves in propria persona in this litigation.

[4] Because of their lengthy titles, for convenience we refer to the two purported causes of action in the complaint as the "intentional infliction" and "negligent infliction" claims, respectively. In so doing, we acknowledge both that a purported claim for negligent infliction is in actuality not a tort separate and apart from the tort of negligence (*Potter v. Firestone Tire & Rubber Co.* (1993) 6 Cal.4th 965, 984), and that courts sometimes choose the acronyms "IIED" and "NIED" to refer to these torts. (See, e.g., *Wooden v. Raveling* (1998) 61 Cal.App.4th 1035; see also *Lawson v. Management Activities, Inc.* (1999) 69 Cal.App.4th 652, 656 [noting that use of acronym for negligent infliction of emotional distress gives "more credence [to the allegation] than it deserves"].)

Plaintiffs alleged that the anonymous threats against them occurred between April and July 2002, while an appeal was pending in unrelated litigation brought by plaintiffs' former employer, Varian Medical Systems (and others), against plaintiffs.[5] The threats alleged in the complaint—most of which were directed solely at Delfino—were either e-mail messages sent to Delfino or were messages posted on the Yahoo! Message Board VAR.[6] Most of the threatening e-mails and postings were sent by an individual using the Yahoo screen name "crack_smoking_jesus"; Moore later admitted to the Federal Bureau of Investigation (FBI) that he had used this pseudonym.[7]

---

[5] The unrelated lawsuit included claims for defamation that arose out of numerous derogatory messages about Varian and certain Varian employees that Delfino and Day posted on Internet message boards. Judgment on a jury verdict adverse to Delfino and Day (i.e., an award of $425,000 in compensatory damages plus punitive damages of $350,000) was entered in that case. Ultimately, the California Supreme Court reversed on the ground that the previous appeal of Delfino and Day from the trial court's order denying their special motions to strike under Code of Civil Procedure section 425.16, subdivision (b)(1) (i.e., their motions to strike the Varian complaint as a "SLAPP" [strategic lawsuit against public participation]) operated as a stay on all further trial court proceedings; accordingly, the Supreme Court determined that the judgment was void. (*Varian Medical Systems, Inc. v. Delfino* (2005) 35 Cal.4th 180.)

[6] It is unnecessary for us to repeat each of the odious e-mail messages and postings attributed to Moore. One posting (by "crack_smoking_jesus") on July 18 read: " 'I arranged for you to have a visitor. Have they [*sic*] been there yet? If not, then they will visit soon. Don't say I didn't warn you. Criminal matters are handled less carefully than civil matters.' " And plaintiffs alleged in the complaint that on July 30, the following e-mail was sent to Delfino (from "dr_dweezil@yahoo.com"): " 'It's 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. I already have proof I was somewhere else. You can look forward to all your fingers getting broken, several kicks to the ribs and mouth, break some teeth, and a cracked head. Also, your car will be trashed and your computer destroyed. Maybe set your place on fire so you can be evicted. If your [expletive] is there, she'll take a little ride to the parts of San Jose where they don't speak [E]nglish . . . Die, [expletive]. You'll wish you had.' "

[7] The attorneys who represented Delfino and Day in the unrelated Varian litigation wrote a law review article about the threatening e-mails and their attempts to trace their origin. (See Eisenberg & Rosen, *Unmasking "crack_smoking_jesus": Do Internet*

The first cause of action of the complaint, captioned "Intentional Infliction of Emotional Distress," alleged that Moore's conduct in sending the anonymous e-mails and postings was intentional and malicious, causing plaintiffs to "suffer humiliation, mental anguish, and emotional and physical distress." Plaintiffs alleged on information and belief that Agilent "was informed and knew that Moore was using its computer system to" send the threatening messages. The second cause of action, captioned, "Negligent Infliction of Emotional Distress," contained (and incorporated by reference) the allegations of the first cause of action.

Agilent filed a motion for summary judgment, or, in the alternative, for summary adjudication. Plaintiffs opposed the motion. On March 18, 2005, the court entered an order granting Agilent's motion for summary judgment, concluding that "Agilent established that it is immune from liability under [title] 47 [of the United States Code section] 230(c)(1) . . . , and plaintiffs failed to raise a triable issue of material fact in regard thereto." Judgment was entered on the summary judgment order on May 13, 2005.[8] Plaintiffs filed a timely notice of appeal from the judgment. The appeal is one that properly lies from a judgment entered upon an order granting summary judgment. (Code Civ. Proc., § 437c, subd. (m); *Oakland Raiders v. National Football League* (2005) 131 Cal.App.4th 621, 628-629.)

Service Providers Have a Tarasoff Duty to Divulge the Identity of a Subscriber Who Is Making Death Threats? (2003) 25 Hastings Comm. & Ent. L.J. 683.)

[8] A separate judgment that is not a subject of the instant appeal was entered on April 19, 2005, in favor of plaintiffs against Moore after a court trial. The judgment consisted of an award of $87,323 in damages collectively to plaintiffs, plus $200,000 (general damages) and $300,000 (punitive damages) awarded to each of the plaintiffs. Although not a default proceeding, Moore did not participate at the trial either personally or through counsel.

DISCUSSION

I. *Issues On Appeal*

Plaintiffs contend that the court erred in granting the summary judgment motion. They assert that Agilent is not immune from suit under section 230 of the CDA. They argue that because Agilent had no CDA immunity and it failed to take measures to protect plaintiffs from Moore's threatening communications, it is subject to negligence liability.

II. *Standard of Review*

As we have acknowledged, "[c]onstruction and application of a statute involve questions of law, which require independent review." (*Murphy v. Padilla* (1996) 42 Cal.App.4th 707, 711; see also *Elene H. v. County of Los Angeles* (1990) 220 Cal.App.3d 1445, 1451 [de novo review of summary judgment motion founded on defense of immunity].) Likewise, since summary judgment motions involve purely questions of law, we review the granting of summary judgment de novo. (*Alexander v. Codemasters Group Limited* (2002) 104 Cal.App.4th 129, 139 [de novo review of "whether a triable issue of material fact exists and whether the moving party was entitled to summary judgment as a matter of law"]; *Chavez v. Carpenter* (2001) 91 Cal.App.4th 1433, 1438.)

III. *The Order Granting Summary Judgment*

A. *Agilent's Motion*

On July 26, 2002,[9] Agilent was contacted by Special Agent Sean Wells from the FBI, who "was requesting information on the user whose originating IP address came back to Agilent for 'dreamcaster.txt.' " Special Agent Wells gave no other information concerning the inquiry during the initial contact. But he followed up with an e-mail to Agilent on July 26, in which he provided a listing of log-in entries for "dreamcaster.txt" where Agilent was the originating IP address; the listing included 25 log-in entries dated

[9] All dates are 2002 unless otherwise stated.

between July 12 and July 15. The internal investigation was handled primarily by Agilent's IT Security Consultant and Program Manager for CITSIRT (Corporate Information Technology Security Incident Response Team), Bill Rolfe, and its EHS & Security Manager, Douglas Buffington.

On July 29, Buffington telephoned Special Agent Wells to introduce himself and to indicate that Agilent would cooperate fully with the FBI. Special Agent Wells stated that he "was investigating some e[-]mail traffic, some of which the FBI suspected might [have been] sent by an Agilent employee." Buffington asked for details but was told that Special Agent Wells had obtained information through a grand jury proceeding and could not discuss any specifics.

On July 30, Rolfe traced "dreamcaster.txt" to the Agilent computer assigned to Moore. Rolfe performed further tests which confirmed that Moore was the current user of the machine. After completing this work, Rolfe e-mailed Buffington on July 30 with the results.

Buffington telephoned Special Agent Wells on July 30 and advised that Agilent had identified the user of the IP address. Before Buffington could identify the person, Special Agent Wells asked, " 'Is the name that you have Cameron Moore?' " Buffington confirmed that this was the case. Special Agent Wells advised Buffington further that (1) "he was investigating complaints by Michelangelo Delfino and Mary Day, who were involved in a lawsuit with their former employer, Varian"; (2) plaintiffs had posted and were continuing "to post tens of thousands of inflammatory messages about Varian executives";[10] (3) after plaintiffs had lost in a jury trial involving Varian, some supporters of Varian began responding negatively to plaintiffs; (4) plaintiffs had learned that Moore had made Internet postings siding with Varian; (5) plaintiffs had made a series of Internet

[10] Delfino testified in deposition that since 1997, he and Day had made over 28,000 Internet postings concerning Varian or Moore.

postings about Moore; (6) plaintiffs "had received some potentially threatening e[-]mails that appeared to come from Moore"; (7) "the situation had 'gotten out of hand' and the FBI wanted 'to put an end to it' "; (8) "the FBI wasn't planning to arrest Moore, didn't consider him to be dangerous, and wasn't after Moore's job"; and (9) the FBI simply wanted to speak to him to "get the situation stopped." Special Agent Wells neither informed Buffington of the substance of any of the e-mails the FBI was investigating, nor advised him that Moore made any threatening postings on Internet bulletin boards. Buffington did not understand from his communications with Special Agent Wells that the e-mails being investigated had been sent by Moore by using Agilent systems to log on to the Internet from work.

On August 1, Special Agent Wells made a follow-up request to Buffington for Agilent to investigate the log-in history (between June 27 and July 10) to determine whether the alias "dr_dweezil2000.txt" also belonged to Moore. Agilent thereafter determined that this alias was also traceable to the Agilent computer assigned to Moore. Buffington informed Special Agent Wells of Agilent's findings.

On August 12, Buffington and Agilent's Management Support Consultant, Stephanie Pierce,[11] met with Moore "to obtain Moore's side of the story and to administer a stern warning." Buffington declared that after Pierce explained what Agilent knew, Moore apologized for involving Agilent "but denied sending any threats through the use of Agilent systems." (Original underscore.) He stated that he had promised in writing that he would not engage in any further similar conduct and thereafter provided Agilent with a copy of his letter to the United States Attorney.[12] Pierce gave Moore a stern

[11] After leaving Agilent in or about May 2003, Stephanie Pierce married and thereafter used Moser as her last name. For clarity and convenience, we refer to the witness by her former surname.

[12] In his lengthy letter to the United States Attorney, Moore admitted guilt, expressed his remorse for the cyberthreats, and presented a detailed account to support his assertion that his actions had been provoked by Delfino's own Internet activity. The

warning; although she indicated that "there was no proof that he had sent threatening e[-]mails over the Internet through the use of Agilent systems, she reminded Moore of Agilent's Standards of Business Conduct[13] and warned him that . . . he should not be using Agilent's computer systems for anything relating to [plaintiffs] or any other personal issues."

In February 2003, Special Agent Wells contacted Buffington to advise him that the FBI planned to arrest Moore for conduct relating to Delfino. Buffington specifically asked if the planned arrest involved conduct by Moore in using Agilent computers, and Special Agent Wells said that it did not involve such conduct. In or about mid-February 2003, the FBI arrested Moore. In late February 2003, Buffington contacted the FBI to request a copy of the affidavit signed by Special Agent Wells pertaining to Moore's arrest (arrest affidavit). Although Buffington was told at the time that the FBI "would be faxing it," he did not receive the faxed copy of the arrest affidavit until April 7, 2003. That arrest affidavit contained a number of details about the substance of Moore's threatening e-mails and postings, none of which had been provided previously by the FBI to Agilent.

---

letter contained no description of the method by which Moore had sent the threatening e-mails and postings, did not indicate that Agilent's computer systems were in any way implicated, and mentioned Agilent only in the following contexts: (1) that Moore was fearful that his actions would result in the loss of his Agilent job; and (2) that some of Delfino's alleged provocative acts involved postings using Moore's name on "Agilent stock message boards [stating] some negative and crude things about [Agilent]."

[13] Agilent's Standards of Business Conduct, under the heading "*May I use Agilent computers . . . for personal messages, personal access to the Internet or other personal use?*" read in part: "[C]ertain messages and materials simply must not be sent or accessed on Agilent equipment or through Agilent systems; these include . . . threatening, sexually explicit or harassing materials. You must not use Agilent resources to create, transmit, store or display messages, images or materials in any of these categories. Misuse of Agilent assets is misconduct and may result in termination of your employment."

On April 22, 2003, Buffington and two other Agilent representatives met with Moore. Moore admitted to Agilent for the first time that "prior to August 2002, he had sent some things that 'weren't nice and could be interpreted as threats' by logging onto the Internet while at work." (Original underscore.) This statement directly contradicted what Moore had told Buffington and Pierce on August 12. Moore denied that he had used Agilent's systems to send any threats after August. He also admitted that he had "sent sexually explicit or offensive e[-]mails over the Agilent e[-]mail system." Moore was informed at the conclusion of the meeting that he "was being placed on immediate administrative leave while Agilent determined what discipline was appropriate."

On April 30, 2003, Agilent terminated Moore's employment. The termination notice advised Moore that he was being involuntarily terminated because he had violated Agilent's Standards of Business Conduct, "specifically misuse of Agilent's assets."[14]

B. *Opposition to Summary Judgment Motion*

The evidence presented in opposition to the summary judgment motion primarily consisted of excerpts from transcripts of the depositions of plaintiffs and several Agilent employees, the arrest affidavit, and documents concerning Moore's sentencing. While that evidence was voluminous, most of it was not germane to the issues of CDA immunity and negligence liability.

Further, while plaintiffs indicated that there was a genuine dispute concerning a number of issues of material fact that Agilent claimed to have been undisputed (UMF), the evidence plaintiffs cited, upon examination, did not support their assertions. For instance, plaintiffs claimed a dispute existed regarding UMF number 7—i.e., that on July

[14] Moore ultimately pleaded guilty in September 2003 to one count of violating section 1512(d)(4) of title 18 of the United States Code (intentional harassment to dissuade another from assisting in a criminal prosecution). (The offense of which Moore was convicted did not involve the use of Agilent's computer system.) He was placed on probation for a period of four years.

30, the FBI neither told Agilent that threats had been sent through Agilent's computer system nor provided it with the contents of any e-mail the FBI was investigating. But plaintiffs' cited evidence consisted of improperly spliced, separate excerpts of Buffington's declaration and the arrest affidavit. As a result of the improper splicing, plaintiffs created purported content that did not exist in either document. (Indeed, the two spliced excerpts of the arrest affidavit were separated by three pages of text.) In any event, the purported evidence plaintiffs cited did not demonstrate that UMF number 7 was disputed.[15]

Other matters raised in plaintiffs' opposition to the summary judgment motion relevant to this appeal are discussed, *post*.

C. *Immunity Under the CDA*

1. *Applicable law*

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 goes on to provide that causes of action inconsistent with it under state law are precluded: "Nothing in this section shall be

[15] There are a number of other instances in which plaintiffs claimed in their response to Agilent's separate statement that material facts were disputed when, in reality, no evidence demonstrating such dispute was cited. These undisputed material facts included the following: (a) the FBI assured Agilent on July 30 that Moore was a threat to no one, that no arrest was planned, and that Agilent need not be concerned about him (UMF no. 6); (b) Agilent's early August internal investigation did not disclose that Moore had used its computer system to send any threatening e-mails or postings (UMF no. 11); (c) when Agilent reprimanded Moore on August 12, he did not admit to using its computer system to make any threatening Internet postings and denied using Agilent's system to send any e-mail threats (UMF no. 13); (d) no Agilent employee knew about, assisted with, participated in, or had any involvement with Moore's cyberthreats (UMF no. 16); (e) Agilent's second internal investigation conducted after Moore's February 2003 arrest did not disclose that Moore had made any cyberthreats (UMF no. 18); and (f) Agilent did not learn the substance of Moore's threatening e-mails and postings until it received the arrest affidavit on April 7, 2003 (UMF no. 19).

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*." (§ 230(e)(3), italics added.)

Agilent contends that CDA immunity applied to plaintiffs' claims here. It argues that plaintiffs sought to impose derivative liability upon Agilent for Moore's Internet communications, where Agilent was simply a provider of an interactive computer service. Plaintiffs naturally dispute this contention.

The CDA—of which section 230 is a part—was enacted in 1996.[16] Its "primary goal . . . was to control the exposure of minors to indecent material" over the Internet. (*Batzel v. Smith, supra,* 333 F.3d at p. 1026.) Thus, an "important purpose of [the CDA] 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 (*Zeran*); see § 230, subd. (b)(4): "It is the policy of the United States—[¶] . . . [¶] (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.") Thus, 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.[17] A second objective of the CDA was to avoid the chilling effect upon

---

[16] Since the passage of the CDA in 1996, "[p]arts of [it] have . . . been struck down as unconstitutional limitations on free speech, see *Reno v. ACLU*, 521 U.S. 844, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997) [concerning constitutionality of portions of section 223]; *United States v. Playboy Ent. Group*, 529 U.S. 803, 120 S.Ct. 1878, 146 L.Ed.2d 865 (2000) [concerning constitutionality of section 561], but the section at issue here, [section] 230, remains intact." (*Batzel v. Smith* (9th Cir. 2003) 333 F.3d 1018, 1026, cert. den. (2004) 541 U.S. 1085.)

[17] "No provider or user of an interactive computer service shall be held liable on account of—[¶] (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious,

Internet free speech that would be occasioned by the imposition of tort liability upon companies that do not create potentially harmful messages but are simply intermediaries for their delivery. (*Zeran, supra*, at pp. 330-331; see also § 230(b): "It is the policy of the United States—[¶] (1) to promote the continued development of the Internet and other interactive computer services and other interactive media; [¶] (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation . . . .")

Zeran, supra, 129 F.3d 327, is the leading case addressing the issue of immunity granted under section 230 to interactive computer service providers.[18] There, the plaintiff (Kenneth Zeran) alleged that America Online, Inc. (AOL) "unreasonably delayed in removing defamatory messages posted by an unidentified third party [on the AOL bulletin board[19]], refused to post retractions of those messages, and failed to screen for

---

filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or [¶] (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph [(A)]." (§ 230(c)(2), fn. omitted.) The end of the actual text of the statute refers to "paragraph (1)." But it is apparent that the reference should be to "paragraph (A)." (See § 230(c)(2), fn. 1.)

[18] Plaintiffs refer repeatedly to a decision critical of *Zeran* by the First District Court of Appeal (Division Two) for which review was subsequently granted by the Supreme Court. (See *Barrett v. Rosenthal* (2004) 114 Cal.App.4th 1379, review granted Apr. 14, 2004, S122953.) Such grant of review by the Supreme Court of course "had the effect of depublishing" the Court of Appeal's decision. (*Quintano v. Mercury Casualty Co.* (1995) 11 Cal.4th 1049, 1067, fn. 6.) Moreover, after oral argument and submission of this case, the Supreme Court, following *Zeran*, reversed the First District Court of Appeal and held that section 230 provides broad immunity from defamation liability for a provider or user of an interactive computer service. (*Barrett v. Rosenthal* (2006) 40 Cal.4th 33.)

[19] An Internet bulletin board is "a computerized version of a cork and pin board on which users can post, read, and respond to messages." (Weber, *Defining Cyberlibel: A First Amendment Limit for Libel Suits Against Individuals Arising from Computer Bulletin Board Speech* (1995) 46 Case Western Reserve L.Rev. 235, 238, fns. omitted.) After logging in to an Internet bulletin board, a person may post messages, respond to

similar postings thereafter." (*Id.* at p. 328.) The anonymous defamatory messages involved the advertising for purported sale of shirts containing "offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City." (*Id.* at p. 329.) The postings included instructions "to call 'Ken,' " and listed the plaintiff's home telephone number. (*Ibid.*) There was no dispute that AOL was an " 'interactive computer service,' "[20] and that the person responsible for the anonymous postings was an " 'information content provider,' "[21] as those terms were defined under the CDA. (*Id.* at p. 330, fn. 2.)

The Fourth Circuit concluded that the CDA provided AOL (as an interactive computer service provider) with immunity from the plaintiff's claims. It reasoned that the CDA's immunity provisions were the result of Congressional recognition of "the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium" (*Zeran, supra,* 129 F.3d at p. 330), and Congress's desire "to encourage service providers to self-regulate the dissemination of offensive material over their services." (*Id.* at p. 331.) The court held that section 230(c)(1) conferred "broad immunity" (*Zeran, supra,* at p. 331) applicable to all interactive computer service

---

messages already posted, or simply read the discussions without posting any messages. (*Id.* at p. 239.) Most Internet bulletin boards permit participants to use pseudonyms. (*Id.* at p. 241.)

[20] Section 230(f)(2)—which, at the time *Zeran* was decided was codified under section 230(e)(2)—provides: "The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."

[21] Section 230(f)(3)—which, at the time *Zeran* was decided was codified under section 230(e)(3)—provides: "The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."

providers, irrespective of whether they were publishers or distributors of the alleged defamatory matter authored by the information content provider. (*Id.* at pp. 331-334.)

At least three other federal circuit courts have followed the Fourth Circuit's decision in *Zeran*, *supra*, 129 F.3d 327. (See *Carafano v. Metrosplash.com, Inc.* (9th Cir. 2003) 339 F.3d 1119; *Batzel v. Smith*, *supra*, 333 F.3d 1018; *Green v. America Online* (3d Cir. 2003) 318 F.3d 465; *Ben Ezra, Weinstein, & Co. v. America Online Inc.* (10th Cir. 2000) 206 F.3d 980.)[22] In addition, two district courts of appeal in California have followed *Zeran*. (See *Gentry v. eBay, Inc.* (2002) 99 Cal.App.4th 816 [Fourth District, Division One]; *Kathleen R. v. City of Livermore* (2001) 87 Cal.App.4th 684 [First District, Division Four].) Moreover, the California Supreme Court has very recently held that *Zeran* properly construed section 230(c)(1) as affording broad immunity to any provider or user of an interactive computer service, irrespective of whether that provider or user may have been viewed under traditional defamation law as a "publisher" or "distributor" (i.e., "secondary publisher") of the allegedly defamatory statement. (*Barrett v. Rosenthal*, *supra*, 40 Cal.4th at pp. 57-58.)

2. *Whether Agilent is immune from suit under the CDA*

There are three essential elements that a defendant must establish in order to claim section 230 immunity. They 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.*, *supra*, 99 Cal.App.4th at p. 830.)

---

[22] The Seventh Circuit Court of Appeals has acknowledged that there is no appellate decision contrary to *Zeran*'s holding that section 230(c)(1) affords immunity to web hosts and other Internet service providers for state-law claims based upon offensive material created by others and published over the Internet. (*Doe v. GTE Corp.* (7th Cir. 2003) 347 F.3d 655, 659-660.) The *Doe* court, however, recognized that there was a theoretical debate on the issue and concluded that it did not need to decide the question. (*Id.* at pp. 660-661.)

We evaluate Agilent's contention that it is immune under the CDA by utilizing this three-factor test.

First: Was Agilent "a provider or user of an interactive computer service?" (*Gentry v. eBay, Inc.*, *supra*, 99 Cal.App.4th at p. 830.) Courts have noted that the CDA has interpreted the term "interactive computer service" broadly. (See, e.g., *Batzel v. Smith*, *supra*, 333 F.3d at p. 1030, fn. 15 [term "includes a wide range of cyberspace services, not only [I]nternet service providers"]; *Optinrealbig.com, LLC v. Ironport Systems, Inc.* (N.D.Cal. 2004) 323 F.Supp.2d 1037, 1044 [term is "broadly defined" under the statute].) Thus, there are a number of examples of the expansive application of "interactive computer service" in determining CDA immunity. (See, e.g., *Gentry v. eBay, Inc.*, *supra*, at p. 831 [online auction Web site]; *Kathleen R. v. City of Livermore*, *supra*, 87 Cal.App.4th at p. 692 [library providing Internet access to public by use of computers]; *Carafano v. Metrosplash.com, Inc.*, *supra*, 339 F.3d at p. 1124 [online dating Web site]; *Batzel v. Smith*, *supra*, at p. 1021 [nonprofit Web site operator]; *Chicago Lawyers' Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc.* (N.D.Ill., Nov. 14, 2006, No. 06 C 0657) ___ F.Supp.2d ___ [2006 WL 3307439] [operator of Internet bulletin board carrying notices of jobs, housing services, and goods for sale]; *Parker v. Google, Inc.* (E.D.Pa. 2006) 422 F.Supp.2d 492, 501 [Internet search engine operator]; *PatentWizard, Inc. v. Kinko's, Inc.* (D.S.D. 2001) 163 F.Supp.2d 1069, 1071 [company providing Internet access to customers through computer rental]; *Schneider v. Amazon.com, Inc.* (2001) 108 Wash.App. 454, 31 P.3d 37, 40-41 [online bookstore Web site].)

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. (See, e.g., Zion, *Protecting the E-*

Marketplace of Ideas by Protecting Employers: Immunity for Employers Under Section 230 of the Communications Decency Act (2002) 54 Fed. Comm. L.J. 493, 496 ["it is evident from the language and legislative history of the [CDA] that Congress intended employers to be covered under § 230," (fn. omitted)]; Garvey, *The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technology* (1999) 25 U. Dayton L.Rev. 133, 139 ["corporations with direct Internet connections are indeed [Internet service providers] and, therefore, should receive [CDA] immunity from employee computer abuse"(fn. omitted)].) Certainly, it is beyond question today—certainly more so than 10 years ago—that "Internet resources and access are sufficiently important to many corporations and other employers that those employers link their office computer networks to the Internet and provide employees with direct or modem access to the office network (and thus to the Internet)." (*American Civil Liberties Union v. Reno* (E.D.Pa. 1996) 929 F.Supp. 824, 832-833, affd. *sub. nom. Reno v. American Civil Liberties Union* (1997) 521 U.S. 844.) And Agilent clearly meets the definition of that term under section 230(f)(2) (see fn. 20, *ante*), in that it "provides or enables computer access by multiple users [i.e., Agilent's employees] to a computer server." As noted in Rolfe's declaration, Agilent's proxy servers are the primary means by which thousands of its employees in the United States access the Internet. In light of the term's broad definition under the CDA, we conclude that Agilent was a provider of interactive computer services. (See, e.g., *Kathleen R. v. City of Livermore*, *supra*, 87 Cal.App.4th at pp. 692-693 [rejecting contention that library was not immune because of its governmental entity status]; *Donato v. Moldow* (2005) 374 N.J.Super. 475, 486-488; 865 A.2d 711, 718 [Web site's noncommercial status and limited use irrelevant to CDA immunity analysis].)

Second: Does "the cause of action treat the defendant [Agilent] as a publisher or speaker of information?" (*Gentry v. eBay, Inc.*, *supra*, 99 Cal.App.4th at p. 830.) On information and belief, plaintiffs alleged that Agilent knew (1) Moore was sending threatening messages, and (2) that he was using Agilent's computer system to send them.

Agilent rebutted this allegation in its summary judgment motion, and plaintiffs presented no evidence in opposition that Agilent had such knowledge. This failing notwithstanding, it is apparent that plaintiffs, in alleging that Moore's employer was liable for his cyberthreats, sought to treat Agilent "as a publisher or speaker" of those messages. (§ 230(c)(1).)

We address whether section 230 immunity may apply to the specific tort claims alleged here. While many of the cases addressing CDA immunity have involved claims for defamation (see, e.g., *Batzel v. Smith*, *supra*, 333 F.3d 1018; *Ben Ezra, Weinstein, & Co. v. America Online Inc.*, *supra*, 206 F.3d 980; *PatentWizard, Inc. v. Kinko's, Inc.*, *supra*, 163 F.Supp.2d 1069; *Blumenthal v. Drudge* (D.D.C. 1998) 992 F.Supp. 44), it is clear that immunity under section 230 is not so limited. The Fourth Circuit noted that "[t]he imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech." (*Zeran*, *supra*, 129 F.3d at p. 330.) Thus, CDA immunity has been applied to defendants asserting that they were interactive computer service providers or users for a variety of tort claims other than defamation. (See, e.g., *Kathleen R. v. City of Livermore*, *supra*, 87 Cal.App.4th 684 [claims included nuisance and premises liability]; *Carafano v. Metrosplash.com, Inc.*, *supra*, 339 F.3d 1119 [claims included invasion of privacy, misappropriation of right of publicity, and negligence]; *Doe v. America Online, Inc.* (Fla. 2001) 783 So.2d 1010 [negligent failure to control third party's illegal postings].) And several cases applying section 230 immunity have involved the specific claim alleged in plaintiffs' complaint here, namely, an intentional infliction claim. (See *Prickett v. InfoUSA* (E.D.Tex. 2006) 2006 WL 887431; *Donato v. Moldow*, *supra*, 865 A.2d 711.)

In *Kathleen R. v. City of Livermore*, *supra*, 87 Cal.App.4th 684, the First District Court of Appeal (Division Four) held that section 230(c)(1) afforded the City of Livermore immunity from a broad array of claims arising out of a public library providing access to the Internet through use of its computers, including a taxpayer action

for waste of public funds (Code Civ. Proc., § 526a), and a claim for violation of substantive due process (42 U.S.C. § 1983). In applying CDA immunity to the taxpayer claim, the court specifically rejected the plaintiff's contention that the defense was limited to tort claims for damages and did not apply to taxpayer actions and suits for declaratory and injunctive relief. (*Kathleen R. v. City of Livermore, supra,* at pp. 697-698; see also *Schneider v. Amazon.com, Inc.*, *supra*, 31 P.3d at 42 ["courts that have considered the question have held § 230 provides immunity to civil claims generally"].) We conclude, therefore, that the claims against Agilent treated it "as a publisher or speaker" (§ 230(c)(1)) of Moore's messages and that plaintiffs' claims were among those to which immunity under the CDA potentially applies.

Third: Was "the information at issue . . . provided by another information content provider?" (*Gentry v. eBay, Inc.*, *supra*, 99 Cal.App.4th at p. 830.)[23] Clearly, Moore was the party who authored the offensive e-mails and postings. The allegations of the complaint do not suggest otherwise; to the contrary, the complaint consistently and repeatedly attributes authorship of the offensive messages to Moore alone. (See, e.g., paragraphs 1, 5, 6, 22, 23, 25 through 28, 30 through 32, 39, 40, 47, and 48 of the complaint.) And there was no evidence that Agilent played any role whatsoever in "the creation or development" of the messages. (§ 230(f)(3); see fn. 21, *ante*.)[24] Clearly,

---

[23] Under the CDA, it is of course possible to be both an interactive computer service provider *and* "an information content provider; the categories are not mutually exclusive." (*Gentry v. eBay, Inc.*, *supra*, 99 Cal.App.4th at p. 833, fn. 11.)

[24] Moreover, even had Agilent played some minor role in the formulation of Moore's messages—a matter unsupported by the evidence here—such conduct would not transform it to the status of an information content provider to defeat CDA immunity. (See *Carafano v. Metrosplash.com, Inc.*, *supra*, 339 F.3d at p. 1124 [interactive dating service not information content provider despite supplying questionnaire used by third party to provide information]; *Ben Ezra, Weinstein, & Co. v. America Online Inc.*, *supra*, 206 F.3d at 985 [AOL, as interactive computer service provider that published allegedly inaccurate stock information created by third party, immune under CDA, notwithstanding AOL advised information content providers on other occasions of inaccuracy of stock

Agilent satisfied the third standard enunciated in *Gentry v. eBay, Inc.*, *supra*, 99 Cal.App.4th at page 830, required for a finding of CDA immunity.

Therefore, the trial court correctly held that Agilent was entitled to CDA immunity, because "(1) [Agilent was] . . . a provider or user of an interactive computer service; (2) the cause of action treat[ed Agilent] as a publisher or speaker of information; and (3) the information at issue [was] provided by another information content provider [Moore]." (*Gentry v. eBay, Inc.*, *supra*, 99 Cal.App.4th at p. 830.) Accordingly, summary judgment was properly granted. (See generally *Salazar v. Upland Police Dept.* (2004) 116 Cal.App.4th 934, 938 [summary judgment appropriate where the defendant establishes immunity defense].)[25]

D. *Intentional Infliction Claim*

We have concluded, *ante*, that summary judgment was properly granted because Agilent was entitled to CDA immunity. But even if plaintiffs' claims were not barred

---

information]; *Barrett v. Rosenthal*, *supra*, 40 Cal.4th at p. 60, fn. 19 ["many courts have reasoned that participation going no further than the traditional editorial functions of a publisher cannot deprive a defendant of *section 230* immunity"].)

[25] We recognize that there is an existing debate concerning whether immunity under the CDA applies equally to both publishers and distributors of information authored by third parties and disseminated over the Internet. (See, e.g., *Doe v. America Online, Inc.*, *supra*, 783 So.2d at pp. 1018-1028 (dis. opn. of Lewis, J.); Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation* (2001) 14 Harv. J.L. & Tech. 569, 637-642; Sheridan, *Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act upon Liability for Defamation on the Internet* (1997) 61 Alb. L. Rev. 147, 167-172.) Our Supreme Court has recently held that a party who distributes a defamatory statement made by a third party over the Internet—even if he or she knows or should know of the statement's defamatory character—enjoys the same CDA immunity from suit as an initial publisher of such a statement. (*Barrett v. Rosenthal*, *supra*, 40 Cal.4th at pp. 57-58.) Thus, under *Barrett*—although Agilent did not act as a distributor of Moore's offensive e-mails and postings, and *at most* merely provided the means of communicating the messages by Moore's use of his employer's computer to access the Internet to send the messages—CDA immunity applies in this instance irrespective of whether Agilent is deemed to have been a publisher or distributor.

under section 230(c)(1), the granting of Agilent's summary judgment motion was nonetheless proper, because plaintiffs failed to make a prima facie showing on their intentional infliction claim against Agilent.

1. *Nature of intentional infliction claim*

To establish an intentional infliction claim, the plaintiff must show " ' "(1) extreme and outrageous conduct by the defendant with the intention of causing, or reckless disregard of the probability of causing, emotional distress; (2) the plaintiff's suffering severe or extreme emotional distress; and (3) actual and proximate causation of the emotional distress by the defendant's outrageous conduct." ' " (*Christensen v. Superior Court* (1991) 54 Cal.3d 868, 903.) "Conduct to be outrageous must be so extreme as to exceed all bounds of that usually tolerated in a civilized community. [Citations.]" (*Davidson v. City of Westminister* (1982) 32 Cal.3d 197, 209.)

It is established that "[o]rdinarily mere insulting language, without more, does not constitute outrageous conduct." (*Cole v. Fair Oaks Fire Protection Dist.* (1987) 43 Cal.3d 148, 155, fn. 7.) Liability based upon an intentional infliction claim " 'does not extend to mere insults, indignities, threats, annoyances, petty oppressions, or other trivialities.' (Rest.2d Torts, § 46, com. d.)" (*Molko v. Holy Spirit Assn.* (1988) 46 Cal.3d 1092, 1122, overruled on another ground in *Aguilar v. Atlantic Richfield Co.* (2001) 25 Cal.4th 826, 854, fn. 19; see also *Fisher v. San Pedro Peninsula Hospital* (1989) 214 Cal.App.3d 590, 617.) But under the circumstances here, Moore's repeated threats of physical harm directed to plaintiffs, stated in graphic terms, were sufficient acts of extreme and outrageous conduct with intent to cause emotional distress. (See, e.g., *KOVR-TV, Inc. v. Superior Court* (1995) 31 Cal.App.4th 1023, 1028-1031 [news reporter's interview of preteen children, including advising them of murder of children's two playmates by playmates' mother and her subsequent suicide, sufficient for finding of outrageous conduct to defeat summary judgment]; *Kiseskey v. Carpenters' Trust for So. California* (1983) 144 Cal.App.3d 222, 229-230 [threats of personal harm, death, and

harm to family if the plaintiff did not sign union agreement constituted outrageous conduct]; but see *Cochran v. Cochran* (1998) 65 Cal.App.4th 488, 494-499 [single telephone message referring to recent sensational airline crash that the plaintiffs interpreted as death threat not outrageous conduct].) Indeed, our Supreme Court has recognized, as a theoretical proposition, that an injurious e-mail communication may give rise to an intentional infliction claim. (*Intel Corp. v. Hamidi* (2003) 30 Cal.4th 1342, 1347.)

But Moore, not Agilent, was indisputably the party who made the threats. Therefore, while it may have been established that *Moore* committed extreme and outrageous acts directed to plaintiffs with the intent to cause emotional distress, there is a significant leap that must occur to establish a prima facie case for an intentional infliction claim *against Agilent*.[26] While plaintiffs' pleading is somewhat uncertain,[27] it appears

---

[26] Citing *Hustler Magazine v. Falwell* (1988) 485 U.S. 46, 56, Agilent argues on appeal that plaintiffs' intentional and negligent infliction claims should be treated as defamation claims. But *Hustler Magazine* is distinguishable and does not support Agilent's assertion here. There, Jerry Falwell sought to recover damages for the publication of an advertisement parody (specifically labeled as such) under theories of invasion of privacy, libel, and intentional infliction. (*Id.* at pp. 47-48.) The jury found against Falwell on the libel claim, but awarded compensatory and punitive damages on Falwell's intentional infliction claim. (*Id.* at p. 49.) The Supreme Court concluded that the intentional infliction award could not stand under the First Amendment, holding that a public figure or public official "may not recover for the tort of intentional infliction of emotional distress by reason of [a satirical] publication[] . . . without showing in addition that the publication contains a false statement of fact which was made with 'actual malice.' " (*Id.* at p. 56.) Here, plaintiffs were not public officials or public figures, did not sue for defamation, and, in pleading the intentional and negligent infliction claims, were not attempting to plead an otherwise defective defamation claim. We therefore reject Agilent's suggestion that we treat plaintiffs' intentional and negligent infliction claims as claims for defamation.

[27] The allegation in the complaint directed toward Agilent reads: "Upon information and belief, at all relevant times, Agilent was informed and knew that Moore was using its computer system to carry out these acts against [p]laintiffs. Agilent failed to terminate Moore's employment, and instead assented to his continued use of its computer system for this unlawful purpose and failed and refused to take measures to

that their contentions are that Agilent should be held liable for Moore's threatening messages (1) because it ratified its employee's actions, (2) under respondeat superior principles, or (3) because Agilent was negligent in its supervision and retention of Moore as its employee. (See *Agarwal v. Johnson* (1979) 25 Cal.3d 932, 947, disapproved on another ground in *White v. Ultramar, Inc.* (1999) 21 Cal.4th 563, 574, fn. 4 [affirming intentional infliction liability of employer for willful acts (utterance of racial epithets and false statements about the plaintiff's job knowledge) of employer's managers]; *Fisher v. San Pedro Peninsula Hospital*, *supra*, 214 Cal.App.3d at p. 618 [employer liable for employee's acts constituting intentional infliction committed within scope of employment].) None of these theories has merit based upon the undisputed evidence presented in the motion.

2. *Ratification*

An employer may be liable for an employee's willful and malicious actions under principles of ratification. (Civ. Code, § 2339; Rest.2d, Agency § 218.)[28] 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 its own. (*Rakestraw v. Rodrigues* (1972) 8 Cal.3d 67, 73; see also Judicial Council of Cal. Civil Jury Instrns. (2006) CACI No. 3710.) The failure to discharge an employee after knowledge of his or her wrongful acts may be evidence supporting ratification. (*Coats v. Construction & Gen. Laborers Local No. 185* (1971) 15 Cal.App.3d 908, 914.)

But here there was no evidence presented in opposition to the motion for summary judgment indicative of Agilent's ratification of Moore's wrongful conduct. The facts as

---

stop [Moore's] activities notwithstanding that they were contrary to Agilent's own corporate policies, thereby ratifying his tortious misconduct."

[28] Employer derivative liability for employee actions need not be founded on respondeat superior, but may be based upon the doctrine of ratification. (*Murillo v. Rite Stuff Foods, Inc.* (1998) 65 Cal.App.4th 833, 852.)

presented in Agilent's motion were that at the time of the initial FBI investigation in late July to mid-August, Agilent (1) had no knowledge of the substance of any e-mail or posting by Moore that was being investigated; (2) was not provided with any details by the FBI about its investigation; (3) was told by the FBI that it was not planning to arrest Moore, that it was "not after Moore's job," that Moore was not a threat to anyone, and that Agilent need not be concerned about him; (4) conducted its own investigation but did not discover evidence that Moore used Agilent's computer systems to send threatening e-mails or Internet postings; and (5) was told by Moore that he had not used Agilent's computer systems to send any threatening e-mails or other messages. It was not until April 7, 2003—through receipt from the FBI of the arrest affidavit—that Agilent learned the content of Moore's threatening e-mails and Internet postings that were alleged to have occurred prior to August. Agilent met with Moore shortly thereafter, at which time Moore admitted for the first time that prior to August 12, he had sent some communications through Agilent's computer systems " 'that could be interpreted as a threat.' " Agilent placed Moore on administrative leave immediately after the interview and terminated him eight days later.

Based upon these undisputed facts,[29] there was no evidence that Agilent, after the fact, treated Moore's malicious conduct as its own. There was thus no triable issue as to plaintiffs' claim that Agilent ratified Moore's tortious actions.

---

[29] While (as we have mentioned in pt. III sec. B, *ante*) plaintiffs claimed in their separate statement in opposition to the motion that a number of these key facts were disputed, a careful review of the supporting and opposing evidence reveals that there was no actual dispute. (See *Uhrich v. State Farm Fire & Cas. Co.* (2003) 109 Cal.App.4th 598, 616-617 [party opposing summary judgment must do more than aver that it has evidence to support cause of action, but must actually present that evidence].) For example, while plaintiffs claimed in their responsive separate statement that a dispute existed regarding UMF number 11 (i.e., that Agilent's August investigation did not disclose that Moore had used Agilent's computer systems to send any threatening e-mails or Internet postings), the evidence plaintiffs cited raised no such dispute. Rather, it consisted primarily of a reference to Pierce's August investigation in which she

3. *Respondeat superior*

We next evaluate plaintiffs' assertion that Agilent should be held liable for Moore's tortious conduct under the doctrine of respondeat superior. Pursuant to this doctrine, "an employer is vicariously liable for his employee's torts committed within the scope of the employment." (*Perez v. Van Groningen & Sons, Inc.* (1986) 41 Cal.3d 962, 967; see also CACI No. 3701.) " 'A risk arises out of the employment when "in the context of the particular enterprise an employee's conduct is not so unusual or startling that it would seem unfair to include the loss resulting from it among other costs of the employer's business. [Citations.] In other words, where the question is one of vicarious liability, the inquiry should be whether the risk was one 'that may fairly be regarded as typical of or broadly incidental' to the enterprise undertaken by the employer. [Citation.]" ' [Citations.]" (*Mary M. v. City of Los Angeles* (1991) 54 Cal.3d 202, 209 (*Mary M.*); see generally 1 Levy et al., Cal. Torts (2006) § 8.03[3][a], pp. 8-19 to 8-20.3.) The plaintiff bears the burden of establishing that the employee's action for which vicarious liability is sought to be imposed was committed within the scope of the employment. (*Ducey v. Argo Sales Co.* (1979) 25 Cal.3d 707, 721.)

Scope of employment in the application of the respondeat superior doctrine has been given a broad construction. (*Farmers Ins. Group v. County of Santa Clara* (1995) 11 Cal.4th 992, 1004 (*Farmers Ins. Group*).) As summarized by our high court: " '[T]he fact that an employee is not engaged in the ultimate object of his employment at the time of his wrongful act does not preclude attribution of liability to an employer.' [Citation.] Thus, acts necessary to the comfort, convenience, health, and welfare of the employee

---

determined that Moore had sent two e-mails (using his own name) to Superior Court Judge Jack Komar and Captain Dennis Bacon in the Santa Clara County Sheriff's office, in which he complained about Delfino's harassment of Moore. Plaintiffs' opposition simply did not present admissible evidence of a dispute as to any matter that demonstrated Agilent's ratification of Moore's conduct.

while at work, though strictly personal and not acts of service, do not take the employee outside the scope of employment. [Citation.] Moreover, ' "where the employee is combining his own business with that of his employer, or attending to both at substantially the same time, no nice inquiry will be made as to which business he was actually engaged in at the time of injury, unless it clearly appears that neither directly nor indirectly could he have been serving his employer." [Citations.]' [Citation.] It is also settled that an employer's vicarious liability may extend to willful and malicious torts of an employee as well as negligence. [Citations.] Finally, an employee's tortious act may be within the scope of employment even if it contravenes an express company rule and confers no benefit to the employer." (*Ibid.*)

But the scope of vicarious liability is not boundless. "[A]n employer will not be held vicariously liable for an employee's malicious or tortious conduct if the employee *substantially* deviates from the employment duties for personal purposes. [Citations.] Thus, if the employee 'inflicts an injury out of personal malice, not engendered by the employment' [citation] or acts out of 'personal malice unconnected with the employment', [citation] or if the misconduct is not an 'outgrowth' of the employment, [citation] the employee is not acting within the scope of employment. Stated another way, '[i]f an employee's tort is personal in nature, mere presence at the place of employment and attendance to occupational duties prior or subsequent to the offense will not give rise to a cause of action against the employer under the doctrine of respondeat superior.' [Citation.] In such cases, the losses do not foreseeably result from the conduct of the employer's enterprise and so are not fairly attributable to the employer as a cost of doing business." (*Farmers Ins. Group*, *supra*, 11 Cal.4th at pp. 1004-1005.)[30]

[30] Thus, in a number of instances, courts have concluded that the employer was not liable for its employee's intentional tort where the employee's act was outside the scope of his or her employment. (See, e.g., *Lisa M. v. Henry Mayo Newhall Memorial Hospital* (1995) 12 Cal.4th 291, 297-299 (*Lisa M.*) [sexual assault by medical technician during

Applying these principles, we find that that Moore's conduct in sending threatening e-mails and postings through the Internet were plainly outside the scope of his employment with Agilent. Even assuming that Moore used Agilent's computer system in accessing the Internet to send one or more of these messages, the injury he inflicted was "out of personal malice, not engendered by the employment." (*Carr v. Wm. C. Crowell Co.* (1946) 28 Cal.2d 652, 656.) Likewise, Moore's messages of hate were not an "outgrowth" of his Agilent employment. (*Id.* at p. 657.) Using Agilent's computer system to log on to a private Internet account to send messages—threatening or otherwise—was never part of Moore's job duties. Indeed, plaintiffs did not dispute this point. Furthermore, the fact that Moore may have been present at the workplace and may have been performing regular employment functions before or after transmitting one or more of the threatening messages do not transform his personal conduct into actions for which Agilent may be held vicariously liable. (*Alma W. v. Oakland Unified School Dist.* (1981) 123 Cal.App.3d 133, 140; see also 2 Dobbs, The Law of Torts, (2001) § 335, pp. 912-913 ["employees may depart from employment without leaving the situs of their work" . . . [¶] . . . [or] by engaging in purely personal acts during working hours"].) As the Supreme Court said in *Lisa M.*, *supra*, 12 Cal.4th at page 306, the employer "may have set the stage for [its employee's] misconduct, but the script was entirely of [the employee's] own, independent invention." Therefore, we conclude that Agilent as a matter of law could not be held vicariously liable for Moore's cyberthreats, because he

---

patient examination]; *Farmers Ins. Group*, *supra*, 11 Cal.4th at pp. 1012-1013 [deputy sheriff's sexual harassment of subordinates]; *Hoblitzell v. City of Ione* (2003) 110 Cal.App.4th 675, 682-686 [city building inspector's harassment of builder, done as favor to inspector's friend]; *Maria D. v. Westec Residential Sec., Inc.* (2000) 85 Cal.App.4th 125 [security guard's sexual assault]; *Borg-Warner Protective Services Corp. v. Superior Court* (1999) 75 Cal.App.4th 1203, 1207-1212 [security guard's arson].)

"*substantially* deviate[d] from the employment duties for personal purposes." (*Farmers Ins. Group, supra*, 11 Cal.4th at p. 1005.)[31]

Moreover, the imposition of vicarious liability upon Agilent for Moore's actions would be inconsistent with the rationale for the respondeat superior doctrine. As our high court has explained, the doctrine is based on "a rule of policy, a deliberate allocation of a risk. The losses caused by the torts of employees, which as a practical matter are sure to occur in the conduct of the employer's enterprise, are placed upon that enterprise itself, as a required cost of doing business." (*Hinman v. Westinghouse Elec. Co.* (1970) 2 Cal.3d 956, 959-960; see also *Johnston v. Long* (1947) 30 Cal.2d 54, 64.) Likewise, "[r]espondeat superior is based on ' "a deeply rooted sentiment" ' that it would be unjust for an enterprise to disclaim responsibility for injuries occurring in the course of its characteristic activities. [Citations.]" (*Mary M., supra,* 54 Cal.3d at p. 208.) We unhesitatingly conclude based upon the circumstances before us—i.e., an employee allegedly using his employer's computer to access his personal Internet account to send anonymous cyberthreats that are unrelated to his employment—that Moore's conduct was not a risk that Agilent bore as part of its enterprise. Agilent thus cannot be held liable for Moore's actions under respondeat superior. (See *Booker v. GTE.Net LLC* (E.D. Ky. 2002) 214 F.Supp.2d 746 [rejecting claim against employer under respondeat superior for employees' creation of fake e-mail address and transmission of e-mail derogatory toward the plaintiff].)[32]

---

[31] We acknowledge that whether the employee's conduct was within the scope of his or her employment is generally a question for the trier of fact. (*Ducey v. Argo Sales Co., supra*, 25 Cal.3d at p. 722.) But where, as here, the undisputed facts demonstrate clearly that an employee's conduct was outside of the scope of his or her employment, the issue is one of law that the court may determine. (*Lisa M., supra*, 12 Cal.4th at p. 299; *Perez v. Van Groningen & Sons, Inc., supra*, 41 Cal.3d at p. 968.)

[32] The district court's holding in *Booker* that the employees' tortious acts were outside the scope of their employment was based upon the conclusion that transmission of the offensive e-mails by means of false third-party e-mail accounts "was most

4. *Negligent supervision/retention*

"An employer may be liable to a third person for the employer's negligence in hiring or retaining an employee who is incompetent or unfit. [Citation.]" (*Roman Catholic Bishop v. Superior Court* (1996) 42 Cal.App.4th 1556, 1564-1565.) Negligence liability will be imposed upon the employer if it "knew or should have known that hiring the employee created a particular risk or hazard and that particular harm materializes." (*Doe v. Capital Cities* (1996) 50 Cal.App.4th 1038, 1054.) As such, "California follows the rule set forth in the Restatement Second of Agency section 213, which provides in pertinent part: 'A person conducting an activity through servants or other agents is subject to liability for harm resulting from his conduct if he is negligent or reckless: . . . [¶] (b) in the employment of improper persons or instrumentalities in work involving risk of harm to others[.]' (*Ibid.*)" (*Evan F. v. Hughson United Methodist Church* (1992) 8 Cal.App.4th 828, 836.) Liability for negligent supervision/retention of an employee is one of direct liability for negligence, not vicarious liability. (2 Dobbs, The Law of Torts, *supra*, § 333, p. 906.)

---

certainly *not* sent in furtherance of [the employer's] business," and was not a matter that was expected in light of the employees' duties. (*Booker v. GTE.Net LLC*, *supra*, 214 F.Supp.2d at p. 750.) Certainly, a number of legal scholars have written on the subjects of employer monitoring of employees' Internet use and potential employer liability for employees' wrongful computer-related activity. (See, e.g., Echols, *Striking a Balance Between Employer Business Interests and Employee Privacy: Using Respondeat Superior to Justify the Monitoring of Web-Based, Personal Employee Electronic Mail Accounts of Employees in the Workplace*, 7 Comp. L. Rev. & Tech. J. 273, 278 (2003); Comment, *I Spy Something Read! Employer Monitoring of Personal Webmail Accounts*, 5 N.C. J. L. & Tech. 121 (2003); Comment, *The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed by Their Employees*, 12 Alb. L.J. Sci & Tech. 683 (2002).) But we note from our research that, somewhat surprisingly, *Booker, supra*, is the only case addressing the issue of the imposition of vicarious liability on an employer based upon employee abuse of the Internet.

Here, plaintiffs alleged that Agilent knew that Moore was using its computer to accomplish his cyberthreats, that it refused to terminate his employment, and that it instead failed to take measures to prevent their recurrence. Plaintiffs' negligent supervision/retention theory fails for at least three reasons.

First, it is doubtful that the record supports a finding of the existence of a legal duty owing to plaintiffs by Agilent. In *Rowland v. Christian* (1968) 69 Cal.2d 108, 113, our Supreme Court enunciated seven factors relevant to determining the existence of duty: "[1] the foreseeability of harm to the plaintiff, [2] the degree of certainty that the plaintiff suffered injury, [3] the closeness of the connection between the defendant's conduct and the injury suffered, [4] the moral blame attached to the defendant's conduct, [5] the policy of preventing future harm, [6] the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach, and [7] the availability, cost, and prevalence of insurance for the risk involved."[33] Applying the first factor, we find that plaintiffs had no business relationship with Agilent. And there is no evidence that Moore's cyberthreats directed toward plaintiffs arose out of, or were in any way connected with his employment. The first *Rowland* factor does not suggest the existence of a duty.

Agilent argues that plaintiffs were not damaged, and plaintiffs admitted that they sought no treatment for their alleged emotional injuries. Plaintiffs argue that the outrageousness of Moore's conduct suggests they were damaged. At best, the second *Rowland* factor neither supports nor opposes a finding of duty.

---

[33] Thus, for instance, the *Rowland* seven-factor test was applied by the court in *Steven F. v. Anaheim Union School Dist.* (2003) 112 Cal.App.4th 904, 915-919, to reach the conclusion that a school district could not be held liable to a student's parents under a negligent supervision theory as a result of the acts of its teacher-employee (i.e., a sexual relationship engaged in by a teacher with a student).

There was little evidence that Agilent's conduct had any "closeness" to plaintiffs' alleged injuries. At most, Agilent supplied Moore with an office computer by which its employee (unbeknownst to Agilent) accessed his personal Internet account and sent threatening messages. Thus, the third *Rowland* factor does not support a finding of duty.

Moreover, the fourth through seventh *Rowland* factors strongly disfavor liability in this instance. There was no "moral blame" in Agilent's conduct evidenced by the record. (See, e.g., *Steven F. v. Anaheim Union School Dist.*, *supra*, 112 Cal.App.4th at p. 917 [no "moral blame" on part of school district in supervision of employee where it provided ongoing awareness programs and extensive employee training].) There is no significant policy of preventing future harm that would result from a finding of duty; indeed, a finding of duty here might have a significant chilling effect upon Internet free speech and might encourage extreme employer oversight of employee activities. (See *id.* at p. 918 [finding duty would turn the culture of the school into "a virtual police state"].) Additionally, the burden imposed on the employer in this instance would be enormous. (See *Macias v. State of California* (1995) 10 Cal.4th 844, 859-860 [in "deciding whether to expand a tort duty of care, courts must consider the potential social and economic consequences"].) It would be a dubious proposition indeed to suggest that a party, simply by virtue of engaging in business, owes a duty to the world for all acts taken by its employee, irrespective of whether those actions were connected with the enterprise in which the business was engaged. (See, e.g., *Mendoza v. City of Los Angeles* (1998) 66 Cal.App.4th 1333, 1341 [no duty by city owed to employee's family member for employee's off-duty criminal acts].) And it is not realistic that the type of risk involved here—unknown malicious acts of an employee bearing no relationship to his job achieved by accessing the Internet to make death threats—is a readily insurable one. Therefore, we conclude that plaintiffs did not establish here that Agilent owed a duty.

Second, even were we to assume the existence of a duty, there was no evidence that Agilent breached any duty of care with respect to the supervision or retention of

Moore as an employee. As we have noted (see pt. III sec. D.2., *ante*), Agilent had no knowledge of the content of any of Moore's threatening e-mails or postings before receiving the arrest affidavit on April 7, 2003. Most important, it was not until the day Moore was placed on administrative leave (leading to his ultimate termination a few days later) that Agilent learned that Moore had used its computer systems to access his personal Internet account to send threatening messages through the Internet more than eight months earlier. Moreover, Agilent's internal investigations—one conducted in August prompted by the FBI's initial inquiry, and the second conducted after Moore's February 2003 arrest—did not yield any information that Moore had used Agilent's computer system to send inappropriate messages over the Internet. Buffington was unable to discover any Internet postings that may have been attributable to Moore. Indeed, plaintiffs—through Delfino's deposition testimony—admitted the impossibility of tracing an anonymous posting to a particular individual. There were thus no facts presented suggesting that Agilent knew or had reason to suspect that Moore was engaged in improper on-the-job conduct. (See *Federico v. Superior Court (Jenry G.)* (1997) 59 Cal.App.4th 1207, 1216 [hairstyling college not liable for employee's molestation of juvenile son of student, where it had no knowledge or notice of inappropriate behavior at work].)

Third, even were we to assume that Agilent (1) knew or should have known that Moore (prior to August) had allegedly used its computers to send threatening e-mails and postings over the Internet, and (2) took no measures to prevent a recurrence of the threats, there was no evidence that Moore in fact used Agilent's system after August to threaten plaintiffs.[34] Thus, any negligent supervision/retention of Moore by Agilent—which alleged negligence, as we have concluded, was devoid of factual support—was not the

[34] The November cyberthreat for which Moore ultimately pleaded guilty indisputably was made without use of Agilent's computer system.

cause of plaintiffs' claimed injuries. (See *Mendoza v. City of Los Angeles*, *supra*, 66 Cal.App.4th at p. 1342 [assuming evidence of negligent hiring, off-duty police officer's killing of fiancé after domestic dispute not caused by such negligence].)

Plaintiffs failed to present evidence supporting their claim based upon the theory that Agilent was negligent in its supervision and/or retention of Moore.[35]

E. *Negligent Infliction Claim*

The second cause of action was captioned as a purported negligent infliction claim. It incorporated by reference all prior paragraphs of the complaint (including the entire intentional infliction claim). As it pertained to Agilent, it contained the same allegations that appeared in the intentional infliction cause of action. (See fn. 27, *ante*.)

As we have noted (see fn. 4, *ante*), there is no independent tort of negligent infliction of emotional distress. (*Potter v. Firestone Tire & Rubber Co.*, *supra*, 6 Cal.4th 965, 984.) Thus, since plaintiffs' purported negligent infliction claim was merely "a species of negligence" (*Wooden v. Raveling*, *supra*, 61 Cal.App.4th 1035, 1046), the better question to ask in appraising plaintiffs' so-called "negligent infliction" allegations is: "What are the circumstances under which a plaintiff can recover damages for emotional distress as a matter of the *law of negligence*?" (*Lawson v. Management Activities, Inc.*, *supra*, 69 Cal.App.4th 652, 657, original italics.)

Using this analytical framework, we have established from our discussion of negligent supervision/retention (see pt. III sec. D.4., *ante*) the nonviability of plaintiffs' purported negligent infliction claim. The claimed negligence pertained to Agilent's retention and supervision of its employee, Moore. As we have discussed, the undisputed evidence showed that plaintiffs did not establish the existence of duty, breach of duty or

---

[35] As is the case with respondeat superior, while we acknowledge that negligent retention is generally a question of fact, it is one of law if no reasonable jury may conclude based upon the undisputed facts that liability exists. (*Federico v. Superior Court (Jenry G.)*, *supra*, 59 Cal.App.4th at p. 1214.)

causation. Accordingly, summary disposition of plaintiffs' purported negligent infliction claim was proper.[36]

DISPOSITION

The judgment entered on the order granting Agilent's motion for summary judgment is affirmed.

Duffy, J.

WE CONCUR:

Bamattre-Manoukian, Acting P.J.

McAdams, J.

[36] For the first time on appeal, plaintiffs argue that Agilent is subject to negligence liability under the theory that—as an extension of the *Tarasoff* (*Tarasoff v. Regents of University of California* (1976) 17 Cal.3d 425) doctrine involving a psychotherapist's duty to warn a potential victim of foreseeable injury caused by a patient—Agilent had a duty to warn plaintiffs under the USA Patriot Act (P. L. 107-56, 115 Stat. 272). We need not address this dubious theory; it is inappropriate for plaintiffs to adopt a new theory for the first time on appeal, and appellate courts will customarily decline to decide such newly minted theories. (*Beroiz v. Wahl* (2000) 84 Cal.App.4th 485, 498, fn. 9; *Mattco Forge, Inc. v. Arthur Young & Co.* (1997) 52 Cal.App.4th 820.)

Trial Court:	Santa Clara County Superior Court No. 1-03-CV-001573
Trial Judge:	Hon. Kevin E. McKenney
For Plaintiffs and Appellants:	Michelangelo Delfino, in pro. per.; Mary E. Day, in pro. per.
Attorneys for Defendant and Respondent:	Bradford K. Newman Katherine C. Huibonhoa Shannon S. Sevey PAUL, HASTINGS, JANOFSKY & WALKER

DELFINO et al. v. AGILENT TECHNOLOGIES
No. H028993