

ILLINOIS OFFICIAL REPORTS
Appellate Court

Lansing v. Southwest Airlines Co., 2012 IL App (1st) 101164

Appellate Court Caption	GREGG LANSING, Plaintiff-Appellant, v. SOUTHWEST AIRLINES COMPANY, a Foreign Corporation, Defendant-Appellee.
District & No.	First District, Sixth Division Docket No. 1-10-1164
Filed	June 8, 2012
Held <i>(Note: This syllabus constitutes no part of the opinion of the court but has been prepared by the Reporter of Decisions for the convenience of the reader.)</i>	The trial court erred in entering summary judgment for defendant in an action alleging defendant was negligent in supervising one of its employees who used defendant's computer, Internet and telephone facilities to harass and threaten plaintiff with e-mails and text messages, notwithstanding defendant's contention that section 230 of the Communications Decency Act gave defendant immunity, since section 230 did not apply where the complaint did not allege defendant was the publisher of its employee's communications, plaintiff alleged defendant failed to address the employee's threats and misuse of his employment after being informed of the misconduct, and the negligent supervision claim did not depend on who published the offensive information.
Decision Under Review	Appeal from the Circuit Court of Cook County, No. 06-L-8221; the Hon. Kathy M. Flanagan, Judge, presiding.
Judgment	Reversed and remanded.

Counsel on Appeal Besetzny Law, P.C. (Kevin S. Besetzny, of counsel), and Leslie J. Rosen, both of Chicago, for appellant.

Matthew T. Walsh and Cozen O'Connor, both of Chicago, for appellee.

Panel JUSTICE LAMPKIN delivered the judgment of the court, with opinion. Presiding Justice R. Gordon and Justice Garcia concurred in the judgment and opinion.

OPINION

¶ 1 Plaintiff Gregg Lansing sued defendant Southwest Airlines Company for negligent supervision of its employee. Plaintiff alleged that he notified defendant that its employee was threatening and harassing him but defendant failed to supervise the employee and take steps to stop his misconduct. The alleged misconduct included the employee's use of defendant's computer, Internet and telephone facilities to send harassing and threatening e-mails and text messages.

¶ 2 The trial court granted summary judgment in favor of defendant based on a finding that section 230 of the Communications Decency Act of 1996 (CDA) (47 U.S.C. § 230 (2000)) afforded defendant immunity from plaintiff's claims that arose from the e-mails and text messages. Plaintiff appealed, arguing that the CDA was inapplicable because his cause of action did not treat defendant as the publisher or speaker of the offensive e-mails and text messages but, rather, was based on defendant's failure to supervise its employee after defendant had received notice of the employee's misconduct.

¶ 3 For the reasons that follow, we reverse the judgment of the trial court.

¶ 4 I. BACKGROUND

¶ 5 In August 2006, plaintiff filed a two-count complaint against defendant Southwest Airlines Company, alleging direct negligence and vicarious liability/ratification. Defendant filed a motion to dismiss the complaint pursuant to section 2-615 of the Code of Civil Procedure (Code) (735 ILCS 5/2-615 (West 2006)) for failure to properly plead a cause of action.

¶ 6 In June 2007, plaintiff filed a first amended complaint, which alleged that defendant: failed to adequately supervise its employee, Thomas McGrew; allowed McGrew to use defendant's computer, Internet and telephone facilities to threaten and harass plaintiff; and failed to take appropriate disciplinary action against McGrew despite notice from plaintiff about McGrew's misconduct.

¶ 7 In February 2008, defendant filed a motion for summary judgment pursuant to section

2-1005(e) of the Code (735 ILCS 5/2-1005(e) (West 2008)), asserting, *inter alia*, that section 230 of the CDA preempted plaintiff's state law claim and gave defendant immunity from liability for plaintiff's alleged negligence claim.

¶ 8 In October 2008, the trial court granted defendant's motion for summary judgment, finding that defendant was afforded immunity under the CDA for the claims arising out of McGrew's use of the Internet because defendant was a provider or user of an interactive computer service and would be deemed the publisher of the harassing e-mails and text messages at issue in plaintiff's cause of action. The trial court noted, however, that the issue of defendant's liability for the harassing telephone calls remained pending.

¶ 9 In December 2008, defendant moved for summary judgment pursuant to section 2-1005(e) of the Code, asserting, *inter alia*, that plaintiff could not prove that McGrew made any threatening telephone calls from one of defendant's telephones or while under the supervision of defendant.

¶ 10 In June 2009, plaintiff filed his second amended complaint, which sought damages against defendant based on its alleged negligent failure—despite repeated notice from plaintiff—to stop McGrew, who was a flight attendant and supervisor employed by defendant, from using his position with defendant and defendant's resources to threaten and harass plaintiff and his friends, family members and professional colleagues. Specifically, plaintiff alleged that McGrew met plaintiff's friend on a Southwest Airlines flight in June of 2004 and then perceived plaintiff as a rival to McGrew's relationship with that friend. McGrew, as defendant's employee, had access to defendant's offices, network, computer terminals, work stations, telephone facilities, customer data information, and business calling cards, and a cell phone provided by defendant.

¶ 11 Plaintiff also alleged that McGrew, from June 2004 through August 2006, used his access to defendant's resources to make harassing telephone calls and send over 1,000 harassing and threatening text messages or e-mails to plaintiff. According to plaintiff, McGrew threatened that, as a supervisor, he knew when people made reservations on his flights and would prevent plaintiff and his family members from flying by placing them on terrorism “no fly” lists with defendant and its affiliated airlines. Further, McGrew emphasized his position and authority with defendant, threatened to “haunt” and “completely ruin” plaintiff, and asserted that no one would believe any complaints plaintiff might lodge against McGrew. As time progressed, McGrew's messages and e-mails became increasingly violent, mentioned plaintiff's family members by name, and were transmitted directly to plaintiff's family members and professional colleagues.

¶ 12 In addition, plaintiff alleged that in April of 2005 and January, March, April and May of 2006, he contacted defendant's customer relations department, reported McGrew's harassment and requested that defendant take measures to stop McGrew's wrongful conduct and harassment. Despite that notice, however, McGrew's wrongful conduct and harassment continued until his employment with defendant was terminated on August 22, 2006. Plaintiff asserted that, as a result of McGrew's conduct and defendant's failure to adequately supervise him, plaintiff changed his telephone number several times in an attempt to avoid McGrew's harassment; was ostracized by his family members, friends and professional

colleagues; and suffered embarrassment, humiliation, distress and anxiety.

¶ 13 In July 2009, defendant filed a motion under section 2-615 of the Code (735 ILCS 5/2-615 (West 2008)) to strike certain allegations and dismiss plaintiff's second amended complaint. Defendant argued that plaintiff ignored the trial court's October 2008 ruling that the CDA preempted plaintiff's claims that arose from the e-mails or text messages McGrew allegedly sent to plaintiff. Defendant also requested sanctions pursuant to Illinois Supreme Court Rule 137 (eff. Feb. 1, 1994), asserting that plaintiff knew his claim of negligent supervision was neither well-grounded in fact nor supported by existing law and included allegations that disregarded the trial court's October 2008 ruling concerning preemption under the CDA.

¶ 14 In August 2009, plaintiff moved the trial court to reconsider its October 2008 ruling about defendant's immunity under the CDA. Plaintiff argued, *inter alia*, that no Illinois state or federal court interpreted the immunity afforded by the CDA so broadly and plaintiff's negligent supervision cause of action did not treat defendant as a publisher of McGrew's e-mails and texts.

¶ 15 In September 2009, the trial court denied plaintiff's motion for reconsideration, granted defendant's motion to strike and dismiss plaintiff's second amended complaint, and denied defendant's motion for Rule 137 sanctions. The trial court granted plaintiff leave to file a third amended complaint.

¶ 16 In November 2009, plaintiff filed a third amended complaint, which made the same allegations that were set forth in his second amended complaint. In the third amended complaint, plaintiff referenced and attached additional exhibits and emphasized certain allegations concerning McGrew's statements about his employment and position with defendant. Plaintiff elected to stand on his third amended complaint.

¶ 17 In April 2010, the trial court held that its October 2008 grant of summary judgment in favor of defendant with regard to the CDA stood as the trial court's ruling on plaintiff's third amended complaint. Accordingly, the trial court entered summary judgment in favor of defendant and against plaintiff on the third amended complaint. The trial court determined that there was no just reason to delay the enforcement or appeal of its summary judgment ruling, and plaintiff timely appealed.

¶ 18 II. ANALYSIS

¶ 19 Before addressing the merits of plaintiff's appeal, we address defendant's argument that plaintiff has failed to preserve for review his argument that his lawsuit is outside the purview of the CDA because it is not based on treating defendant as the publisher of the offensive material but, rather, is based on defendant's failure to act on plaintiff's complaints about its employee's misconduct.

¶ 20 Defendant's argument lacks merit. According to the record, plaintiff's amended complaints clearly asserted as the basis of his negligent supervision claim defendant's failure to supervise its employee and stop his campaign against plaintiff after plaintiff had notified defendant of the employee's harassing and threatening conduct. Plaintiff also argued this claim to the trial court below in response to defendant's motion for summary judgment.

Contrary to defendant’s assertion on appeal, plaintiff’s motion for reconsideration did not raise a new argument but, rather, reiterated the basis of his claim against defendant as pled in his amended complaint and argued that the trial court erroneously extended the CDA’s immunity provision to bar plaintiff’s pled claim.

¶ 21 We review *de novo* the trial court’s grant of summary judgment. *Anderson v. Alberto-Culver USA, Inc.*, 317 Ill. App. 3d 1104, 1110 (2000). Summary judgement is a “drastic means of disposing of litigation and therefore should be allowed only when the right of the moving party is clear and free from doubt.” *Purtill v. Hess*, 111 Ill. 2d 229, 240 (1986). “In determining a summary judgment motion, the pleadings, affidavits, depositions and admissions on file must be construed strictly against the moving party and liberally in favor of the opponent.” *Anderson*, 317 Ill. App. 3d at 1110. Reversal of a grant of summary judgment is warranted where, on review, a material issue of fact or an inaccurate interpretation of law exists. *Id.*

¶ 22 In a cause of action for negligent supervision, the plaintiff must establish that (1) the employer had a duty to supervise its employee; (2) the employer negligently supervised its employee; and (3) such negligence proximately caused the plaintiff’s injuries. *Mueller v. Community Consolidated School District 54*, 287 Ill. App. 3d 337, 342-43 (1997). The existence of a duty is a question of law for the court to decide, and the issues of breach and proximate cause are questions of fact for the trier of fact, provided that there is a genuine issue of material fact regarding those issues. *Anderson*, 317 Ill. App. 3d at 1111.

¶ 23 Defendant contends that subsection 230(c)(1) of the CDA (47 U.S.C. § 230(c)(1) (2000)) renders it immune from liability in plaintiff’s negligent supervision cause of action. The trial court granted defendant’s motion for summary judgment, finding that the CDA protected defendant from liability as a matter of law. Plaintiff argues that any immunity under subsection 230(c)(1) of the CDA does not apply to his negligent supervision cause of action and that, even if it did, defendant does not meet the terms to qualify for such immunity.

¶ 24 Section 230 of the CDA, which is entitled “Protection for private blocking and screening of offensive material,” protects certain Internet-based actors from certain kinds of lawsuits. 47 U.S.C. § 230 (2000). When Congress enacted section 230 of the CDA, it found that the rapidly developing array of Internet and other interactive computer services flourished, to the benefit of all Americans, with a minimum of government regulation and Americans increasingly relied on interactive media for a variety of political, educational, cultural and entertainment services. 47 U.S.C. § 230(a) (2000). While Congress sought to promote the continued development of the Internet and preserve the free market that existed on it, Congress also wanted to encourage the development of technology that maximized user control over the information that individuals, families and schools received on the Internet, including technology that empowered parents to restrict their children’s access to objectionable or inappropriate online material. 47 U.S.C. § 230(b) (2000).

¶ 25 Accordingly, Congress provided, under subsection (c), which is entitled “Protection for ‘Good Samaritan’ blocking and screening of offensive material,” as follows:

“(1) Treatment of publisher or speaker

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.

(2) Civil liability

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, 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 (1).” 47 U.S.C. § 230(c) (2000).

An interactive computer service provider must, when it enters an agreement with a customer for the provision of interactive computer service, notify the customer that parental control protections are commercially available. 47 U.S.C. § 230(d) (2000).

¶ 26 Concerning its effect on other laws, section 230 of the CDA shall not be construed to: impair the enforcement of any federal criminal statute and certain specified federal statutes that concern the prohibition of obscene or harassing telephone calls, the restriction of children’s access to harmful material on the World Wide Web, obscenity, and sexual exploitation of children (47 U.S.C. § 230(e)(1) (2000)); limit or expand any law pertaining to intellectual property (47 U.S.C. § 230(e)(2) (2000)); limit the application of the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510 (2000)) or any similar state law (47 U.S.C. § 230(e)(4) (2000)); or prevent any state from enforcing any state law that is consistent with section 230 (47 U.S.C. § 230(e)(3) (2000)). Furthermore, “[n]o cause of action may be brought and no liability may be imposed under any state or local law that is inconsistent with [section 230].” 47 U.S.C. § 230(e)(3) (2000).

¶ 27 “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.” 47 U.S.C. § 230(f)(2) (2000).

¶ 28 “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.” 47 U.S.C. § 230(f)(3) (2000).

¶ 29 When interpreting a federal statute, state courts should generally follow the decisions of federal courts to ensure that the statutory scheme is uniformly applied. *Wilson v. Norfolk & Western Ry. Co.*, 187 Ill. 2d 369, 374 (1999). When federal cases conflict or are inconsistent with respect to a given proposition, and no United States Supreme Court case directly addresses the issue, we will follow the decision that is more “reasonable and logical” and more consistent with both the statutory purpose and Supreme Court precedent. *Id.* at 381-82. Also, because Illinois federal district courts are bound by Seventh Circuit precedent, we tend to give greater weight to Seventh Circuit cases to “avoid[] the anomalous situation of two

contrary results being obtainable depending on where the case is filed in Illinois.” *Id.* at 383 (“[W]ere we to adopt a rule contrary to that of the Seventh Circuit, *** the viability of a claim [under a given federal statute] could turn on whether the action was filed in federal or state court.”). These are not unyielding rules, however; where there is a split of authority among the federal circuit courts of appeal and the Supreme Court has not ruled on the issue, we are not required to follow federal cases, even those from the Seventh Circuit, that appear wrongly decided. *Bowman v. American River Transportation Co.*, 217 Ill. 2d 75, 91 (2005).

¶ 30 In analyzing the scope of section 230(c)(1), the plain meaning of the statute is conclusive unless the literal application of the statute will produce a result demonstrably at odds with the intentions of its drafters. See *United States v. Balint*, 201 F.3d 928, 932-33 (7th Cir. 2000). “We look beyond the express language of a statute only where such language is ambiguous, or where a literal interpretation would lead to absurd results or thwart the goals of the statutory scheme.” *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Lauer*, 49 F.3d 323, 326-27 (7th Cir. 1995). A court’s interpretation is guided not just by a single sentence or clause, but by the language of the whole law and its policy. *Balint*, 201 F.3d at 932-33.

¶ 31 Defendant contends that it is entitled to immunity under the CDA from plaintiff’s cause of action because (1) defendant is afforded broad immunity as a provider or user of an interactive computer service (ICS); (2) plaintiff’s cause of action treats defendant as the publisher or speaker of the offensive communications; and (3) a third party, McGrew, authored the offensive communications.

¶ 32 A. Providers or Users of an Interactive Computer Service

¶ 33 First, we consider whether defendant qualifies as a provider or user of an ICS, which term is defined in section 230(f)(2) of the CDA. Plaintiff argues that defendant is a commercial air travel provider, not an Internet service provider, and when Congress enacted the CDA in 1996, it did not intend to include within the concept of an ICS employers who gave their employees access to the Internet for the purpose of their work. In 1996, employers did not utilize the Internet in their day-to-day operations, and the language of the CDA, according to plaintiff, indicates that it was originally tailored for traditional providers of Internet and e-mail services, such as AOL, CompuServe, Prodigy and Earthlink.

¶ 34 Defendant responds that the history surrounding the CDA indicates that Congress intended to protect all Internet service providers, including employers because they provide a “front end to the Internet.” Defendant cites a statement in the Congressional Record that was made when section 230 was offered as an amendment to the proposed CDA. Specifically, Representative Christopher Cox explained that the amendment would accomplish two things. In addition to establishing the policy that Congress did not want the federal government to regulate Internet content, the amendment would also:

“protect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet, let us say, who takes steps to screen indecency and offensive material for their customers. It will protect them from taking on liability.” 141 Cong. Rec. H8460-01, at 8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

Defendant also cites the conference report, which commented that the Good Samaritan

protections from civil liability in section 230 of the CDA applied to all interactive computer services, “including non-subscriber systems such as those operated by many businesses for employee use.” H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 124, 208.

¶ 35 The parties’ arguments concerning the term *Internet service provider*, which is neither defined nor mentioned in section 230 of the CDA, are irrelevant to the issue before this court. The proper focus of the analysis is whether defendant is a user or provider of an *interactive computer service* as defined in section 230(f)(2) of the CDA. See *Batzel v. Smith*, 333 F.3d 1018, 1030-31 (9th Cir. 2003).

¶ 36 We find that, under the plain language of the statute and its broad definition of an ICS, an employer like defendant qualifies as a provider or user of an ICS because defendant uses an information system or service that multiple users, like defendant’s employees, use to access the Internet. See 47 U.S.C. § 230(f)(2) (2000). See also *Delfino v. Agilent Technologies, Inc.*, 52 Cal. Rptr. 3d 376, 389-90 (Cal. Ct. App. 2007) (corporate employer that gave its employees Internet access was an ICS provider); *Kathleen R. v. City of Livermore*, 104 Cal. Rptr. 2d 772, 777 (Cal. Ct. App. 2001) (library providing Internet access to the public by use of computers qualified as an ICS provider or user).

¶ 37 B. Subsection 230(c)(1) and Broad Immunity

¶ 38 Defendant contends that subsection 230(c)(1) of the CDA grants an ICS user or provider broad immunity from any potential liability that is derived from content posted on or transmitted over the Internet by a third party. Defendant’s contention has support in other state courts and federal circuits. See *Delfino*, 52 Cal. Rptr. 3d at 390 (“it is clear that immunity under section 230” applies to a variety of tort claims other than defamation); *Universal Communication Systems, Inc. v. Lycos, Inc.*, 478 F.3d 413, 419 (1st Cir. 2007) (In light of section 230’s policy concerns, the court found that “section 230 immunity should be broadly construed.”); *Batzel v. Smith*, 333 F.3d 1018, 1031 n.19 (9th Cir. 2003) (describing section 230 as creating a “broad immunity”); *Ben Ezra, Weinstein, & Co. v. American Online Inc.*, 206 F.3d 980, 984-85 (10th Cir. 2000) (section 230 “creates a federal immunity to any state law cause of action that would hold computer service providers liable for information originating with a third party”); *Zeran v. America Online, Inc.*, 129 F.3d 327, 328-30 (4th Cir. 1997) (“By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.”).

¶ 39 Other courts, however, disagree with or question the proposition that subsection 230(c)(1) provides such broad immunity from liability deriving from third-party content. *City of Chicago v. Stubhub!, Inc.*, 624 F.3d 363, 366 (7th Cir. 2010) (“subsection (c)(1) does not create an ‘immunity’ of any kind”); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100 (9th Cir. 2009) (“Looking at the text [of subsection (c)(1)], it appears clear that neither this subsection nor any other declares a general immunity from liability deriving from third-party content ***.”); *Chicago Lawyers’ Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 669-71 (7th Cir. 2008) (questioning whether subsection 230(c)(1) creates any form

of immunity); accord *Doe v. GTE Corp.*, 347 F.3d 655, 660 (7th Cir. 2003).

¶ 40

We agree with the analysis of the Seventh Circuit that section 230(c) “as a whole cannot be understood” as granting blanket immunity to an ICS user or provider from any civil cause of action that involves content posted on or transmitted over the Internet by a third party. *Craigslist, Inc.*, 519 F.3d at 669, 671. Neither section 230’s title (“Protection for private blocking and screening of offensive material”) nor subsection (c)’s caption (“Protection for ‘Good Samaritan’ blocking and screening of offensive material”) suggests that section 230 provides immunity for a negligence action based upon the defendant’s failure to supervise its employee. The Seventh Circuit noted that the caption of section 230(c) refers simply to protections for those who block and screen offensive material and the text of subsection 230(c)(1) does not mention *immunity* or any synonym. *GTE Corp.*, 347 F.3d at 659-60. Moreover, the statutory goal of encouraging the filtering and screening of offensive material would be undermined if ICS users and providers could expect immunity even if they were indifferent to the content of the information they hosted or transmitted. *GTE Corp.*, 347 F.3d at 659-60 (it is unlikely that, when Congress enacted the CDA to protect Good Samaritans from liability for filtering offensive content, Congress also intended to grant broad immunity to ICS users or providers that did not screen any third-party content whatsoever). See also *Chicago Lawyer’s Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 461 F. Supp. 2d 681, 695-96 (N.D. Ill. 2006) (Congress enacted 230(c) to overrule *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), which held that the provider of an online messaging board became a publisher when it deleted some offensive third-party postings and, thus, was subject to publisher’s liability for the defamatory postings it failed to remove).

¶ 41

Defendant’s interpretation of subsection 230(c)(1) expands its scope beyond its language. We, like the Seventh Circuit, read subsection 230(c)(1) to do exactly what it says, and what it says is that an ICS user or provider like defendant must not “be treated as the publisher or speaker of any information provided by” someone else. 47 U.S.C. § 230(c)(1) (2000); see *Craigslist, Inc.*, 519 F.3d at 671. Accordingly, because subsection 230(c)(1) limits who may be called the publisher or speaker of information that appears online, it could foreclose any liability that depends on deeming the ICS user or provider a publisher or speaker, like a cause of action for defamation, obscenity, or copyright infringement. See *GTE Corp.*, 347 F.3d at 659-60; *Stubhub!, Inc.*, 624 F.3d at 366.

¶ 42

The CDA was not enacted to be a complete shield for ICS users or providers against any and all state law torts that involve the use of the Internet. Such an overly broad interpretation of the CDA is inconsistent with the statutory purpose to encourage the restriction of objectionable or inappropriate online material. Moreover, such a grant of blanket immunity would lead to the anomalous result that occurred in the trial court below, *i.e.*, plaintiff was allowed to proceed with his negligent supervision claim against defendant where the evidence of the employee’s threatening and harassing conduct arose from telephone calls, but that same cause of action was barred where the evidence of the very same wrongful conduct arose from e-mails and text messages. The CDA does not bar plaintiff’s cause of action simply because defendant’s employee used the Internet access provided by defendant as one vehicle to harass and threaten plaintiff.

¶ 43 For purposes of defendant’s summary judgment motion, the parties agree that defendant’s employee McGrew created the e-mails and text messages that were sent over the Internet. We conclude, accordingly, that subsection 230(c)(1) of the CDA merely entitles defendant not to be “the publisher or speaker” of those e-mails and text messages. 47 U.S.C. § 230(c)(1), (f)(3) (2000). The remaining issue, then, is whether plaintiff’s cause of action treats defendant as the publisher or speaker of the offensive information.

¶ 44 C. Treatment as a Publisher or Speaker

¶ 45 We find that section 230(c) of the CDA does not apply to plaintiff’s negligent supervision cause of action because any issue concerning whether defendant acted like a publisher or speaker of the offensive material is irrelevant to plaintiff’s pled claim. Plaintiff’s negligent supervision cause of action does not require publishing or speaking as a critical element, and holding defendant liable for its failure to supervise its employee after defendant had received notice of the employee’s wrongful conduct does not treat defendant as if it were the publisher or speaker of the alleged e-mails and texts.

¶ 46 Under the CDA, “what matters is not the name of the cause of action—defamation versus negligence versus intentional infliction of emotional distress—what matters is whether the cause of action inherently requires the court to treat the defendant as the ‘publisher or speaker’ of content provided by another.” *Barnes*, 570 F.3d at 1101-02. In *Barnes*, the plaintiff sued Yahoo!, Inc., an Internet service provider, for negligent undertaking and promissory estoppel based on Yahoo’s failure to remove indecent profiles of the plaintiff that were posted on Yahoo’s Web site by the plaintiff’s former boyfriend. The court held that the CDA barred the plaintiff’s negligent undertaking claim because it was based on Yahoo’s failed undertaking to remove or depublish the offensive profiles and, thus, was based on a violated duty that was derived from Yahoo’s conduct as a publisher. *Id.* at 1103. However, the court held that the CDA did not bar the plaintiff’s promissory estoppel claim because it was based on a violated duty that sprang from an enforceable promise Yahoo had breached, *i.e.*, Yahoo’s promise to the plaintiff to promptly remove the offensive material from its Web site. *Id.* at 1107-08.

¶ 47 Here, the duty that plaintiff alleges defendant has violated is derived from defendant’s duty to supervise McGrew’s conduct as an employee of defendant. Defendant’s duty to supervise its employee is distinct from any conduct like editing, monitoring or removing offensive content published on the Internet. Contrary to defendant’s argument on appeal, plaintiff’s theory of liability is not based on defendant allowing McGrew access to the Internet to publish inappropriate and defamatory electronic messages and then failing to either monitor his messages or prevent them from being sent or somehow remove them. Rather, plaintiff, seeks to hold defendant liable for failing to investigate plaintiff’s complaint about McGrew’s wrongful conduct, reprimand him, and timely suspend or terminate his employment. Specifically, plaintiff alleged that he repeatedly notified defendant that McGrew was using his position of employment with defendant and defendant’s equipment and resources to harass and threaten plaintiff and his family, friends, and professional colleagues. Clearly, the duty plaintiff alleges defendant violated is not derived from any

behavior by defendant that is similar to publishing or speaking.

¶ 48 To support his argument that plaintiff's claim is barred by the CDA, defendant cites *Delfino*, 52 Cal. Rptr. 3d 376. In *Delfino*, the plaintiffs received anonymous threatening messages that were sent over the Internet and were eventually traced by the FBI to an employee of the defendant, a technology corporation. The defendant cooperated with the FBI to determine the origin of the offensive communications, conducted its own internal investigation to determine whether its employee had made any cyberthreats to the plaintiffs, placed the employee on administrative leave while the matter was investigated, and then terminated the employee when he admitted that he may have sent offensive messages by logging onto the Internet at work. *Id.* at 385. The plaintiffs sued the defendant and the employee, alleging intentional and negligent infliction of emotional distress, ratification, *respondeat superior*, and negligent supervision/retention of an employee. The reviewing court affirmed the trial court's grant of summary judgment in favor of the defendant, holding that the defendant was entitled to CDA immunity because it was an ICS and the plaintiffs' cause of action treated the defendant as the speaker or publisher of its employee's cyberthreats. *Id.* at 392.

¶ 49 The *Delfino* court also held that, "even if plaintiffs' claims were not barred under section 230(c)(1)" of the CDA, summary judgment was nonetheless proper because the plaintiffs failed to make a *prima facie* showing on their claims against the defendant. *Id.* Relevant to the appeal before us, the *Delfino* court found the plaintiffs' negligent supervision theory of liability failed because the existence of a legal duty owed to the plaintiffs was doubtful where there was no evidence that the employee's cyberthreats were in any way connected with his employment. *Id.* at 398. Furthermore, the facts did not suggest that the defendant knew or had reason to suspect that its employee was engaged in improper on-the-job conduct. *Id.* at 399. In addition, there was no evidence that the employee used the defendant's computer system to threaten the plaintiffs after the defendant conducted its internal investigation. *Id.*

¶ 50 As discussed above, we do not follow the holdings of the courts that have interpreted section 230(c)(1) as granting blanket immunity to an ICS user or provider from any cause of action involving content posted on or transmitted over the Internet by a third party. In *Delfino*, the court's analysis of the scope of immunity under section 230(c)(1) was primarily confined to the context of the plaintiffs' intentional and negligent infliction of emotional distress claims, which were similar to claims for defamation and did seek to hold the defendant liable for conduct derived from the publication of the offensive information. Accordingly, *Delfino*'s conclusion that the CDA's immunity bars a negligent supervision claim lacks analysis and is not persuasive. Finally, *Delfino*'s alternative analysis concerning the plaintiffs' failure to make a *prima facie* showing to support their negligent supervision claim is not relevant to the appeal before us. The facts pled by plaintiff do not treat defendant as the publisher of McGrew's communications, and plaintiff has alleged that defendant, unlike the employer in *Delfino*, failed to take any action to address its employee's threats and misuse of his position of employment after plaintiff had informed defendant about the employee's misconduct.

¶ 51 Subsection (c)(1) of the CDA limits who may be called the publisher of information that appears online, and plaintiff's negligent supervision cause of action does not depend on who

published McGrew's offensive information. Consequently section 230(c) of the CDA does not bar plaintiff's cause of action.

¶ 52

III. CONCLUSION

¶ 53

We reverse the trial court's award of summary judgment in favor of defendant and remand for further proceedings.

¶ 54

Reversed and remanded.