

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

E360INSIGHT, LLC,

Plaintiff,

v.

COMCAST CORPORATION,

Defendant.

No. 08 C 340  
Judge James B. Zagel

**MEMORANDUM OPINION AND ORDER**

Plaintiff e360Insight, LLC is a marketer. It refers to itself as an Internet marketing company. Some, perhaps even a majority of people in this country, would call it a spammer. e360 sends e-mail solicitations and advertisements, for a fee, to millions of e-mail users. More than a few of those users are subscribers to Comcast, an Internet service provider. Many e-mail users do not want to see (or delete unread) the messages sent by e360. Even if every user wanted these e-mails, Comcast might well have its network overloaded by the mailings. Comcast, like the federal judiciary and other enterprises, uses filters to control the volume of its e-mail and to block e-mails its users don't want to see.

It can fairly be said that there is a national discussion about blocking unwanted messages of all sorts. In 2004, Congress noted that unsolicited commercial e-mail is currently estimated to account for over half of all e-mail traffic and noted, too, that these e-mails imposed significant costs on those who carry and receive such e-mail. 15 U.S.C. § 7701 (a)(2), (6) (2004). This is the context of this case. There is a "do not call list" designed to stop unsolicited phone calls and faxes. Many, if not most, large companies, block messages to their own employees. On the other hand, there are no laws which facilitate the blocking of direct mail solicitations through the

post office or package carriers, perhaps because the cost of physical delivery of a paper solicitation significantly limits its use. The idea of blocking seems at odds in some way with free speech protection, even though there are limits imposed on the free speech protection of commercial speech, which is, I infer, the principal, if not the only, business of e360. None of the larger policy issues, though, is particularly relevant to the decision of Comcast's motion for judgment on the pleadings.

The claims here are four: (1) a federal law claim for violation of the Computer Fraud and Abuse Act (CFAA); (2) a claim of infringement of free speech in violation of First Amendment rights; (3) a state law claim for tortious interference with prospective economic advantage; and (4) a claim for deceptive or unfair practices barred by the Illinois Consumer Fraud Act (ICFA). The motion for judgment on the pleadings argues that the Communications Decency Act of 1996 (CDA) protects Comcast from these claims even if they would otherwise be valid.

It is clear that Congress understood that it would not be enough to pass a law against mass electronic mailings. It knew that servicers like Comcast would create software to identify, filter, and block e-mail messages that were unwanted. It knew, too, that the details of such software could not be publicly disclosed, so as to prevent them from being easily evaded. The policy was to make it easier for e-mail recipients to control the information they receive, particularly the material received by minors at home and in schools.

Congress, and, I think, everyone else who studied the issue understood that blocking software would probably block too much. To insure that you or your child will not receive unwanted or inappropriate e-mails, your Internet service may wind up preventing you from receiving some e-mails that are neither unwanted nor inappropriate. Such Internet service

providers feared they might be held liable for blocking too much, or even too little, and this was, as Congress recognized, “[a] disincentive[ ] for the . . . utilization of blocking and filtering technologies.” 47 U.S.C. § 230(b)(4) (1998). So, Congress passed the so-called Good Samaritan provision of the CDA to protect providers who take actions to prevent access to objectionable content:

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 . . . objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable . . . the technical means to restrict access.

§ 230(c)(2). The Act of Congress expressly pre-empted state or local laws inconsistent with its grant of immunity. § 230(e).<sup>1</sup>

The claim that a suit is barred by federal statute may be properly raised in a motion for judgment on the pleadings. *See McCready v. eBay, Inc.*, 453 F.3d 882 (7th Cir. 2006); *Chicago Lawyers Comm. for Civil Rights v. Craigslist, Inc.*, 461 F.Supp.2d 681 (N.D. Ill. 2006), aff’d, 2008 WL 681168 (7th Cir. 2008) (claim for *failure* to block).

The initial question is whether the kind of unsolicited and bulk e-mails (whether you call them spam or mass marketing mailings) are the sort of communications an entity like Comcast could deem to be objectionable. A few courts have addressed the issue and answered “yes.” *See Optinrealbig.com, LLC v. Ironport Systems, Inc.*, 323 F.Supp.2d 1037 (N.D. Cal. 2004) (company that forwarded spam complaints to ISPs entitled to immunity). Indeed, section 230

---

<sup>1</sup>In this case, Congressional policy does not differ, much, if at all, from Illinois law. See 815 ILCS 511/10 (Electronic Mail Act) which permits providers to block receipt or transmission of unsolicited advertisements on their own initiative and states that providers shall not be held liable for such actions taken in good faith.

imposes a subjective element into the determination of whether a provider or user is immune from liability. *Zango, Inc. v Kaspersky Lab, Inc.*, No. 07-0807, slip. op. at 6-7 (W.D. Wash. Aug. 28, 2007) (noting that section 203(c)(2) only requires that the provider subjectively deems the blocked material objectionable); *Pallorium v. Jared*, 2007 WL 80955, at \*7 (Cal. Ct. App. Jan. 1, 2007) (same). This standard furthers one of section 230's goals "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services." § 230(b)(3). Here, there is no question that Comcast, through the use of its numerous programs, software, and technologies, considers the material sent by e360 via e-mail objectionable.

e360 argues that § 230(c) has a narrower ambit than the one claimed by Comcast. e360 insists that a broad immunity was enacted, but not so broad as to protect Comcast. It relies on *Chicago Lawyers' Committee*, but it is difficult to determine what language in *Chicago Lawyers' Committee* favors e360. 461 F.Supp.2d 681. The problem the Court of Appeals confronted in that case and in *Doe v. GTE*, 347 F.3d 655 (7th Cir. 2003), was the problem of the service provider who did not block anything, or anything much. The question before the Courts there was how to read a statute which seemed to offer protection to providers who did block, a protection which was intended to be an incentive to block. Should the statute be extended to protect those who choose to do nothing? Implicit in both decisions is the conclusion that the statute does provide fairly absolute protection to those who choose to block. This was the choice Comcast made.

The validity of that choice is attacked by the claim, presumed true, that e360 is in compliance with another federal act, 15 U.S.C. §§ 7701-7713 (2004) (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) (CAN-SPAM).

e360 rejects the spammer characterization, saying that it sends e-mails only to persons who opt-in with e360 (or its partners) to receive e-mails. It has a common practice of sending e-mails to request a second confirmation of willingness to receive e-mails. Beginning in 2005, Comcast began a program of indiscriminate blocking of e360 e-mails, which is a significant problem for e360 because, for the majority of its addressees, it has no other way to deliver its goods. e360 protested and, sometimes, Comcast would release a block after hearing from e360 that it was mailing to people who were willing recipients. By 2007, Comcast refused any further releases and showed little interest in discussing the matter with e360.<sup>2</sup>

But compliance with CAN-SPAM, Congress decreed, does not evict the right of the provider to make its own good faith judgment to block mailings. Section 7707 of the Act says that nothing in the Act shall “have any effect on the lawfulness . . . under any other provision of

---

<sup>2</sup>e360 says, in its brief, that Comcast has also engaged in “denial of service” attacks on their system which acts overwhelm e360's system and prevent it from sending or receiving e-mails. e360 also claims that Comcast sends incorrect bounce information to their system with respect to e-mail addresses of those on e360's opt-in list. I do not understand what is being alleged. If e360 means that Comcast is refusing to transmit the e-mails and communicates this fact to e360 by bouncing them back, then it is e360's choice to submit very large numbers of e-mails for transmission which, after the first Comcast block, it should have known of this possibility and been prepared for it (perhaps by altering its protocols to allow for a connection to be disconnected). It is hard to see that sending e-mails back, in this context, is a denial of service “attack” when it is designed to prevent legitimate users of a service from using the service. It is not an “attack” to prevent users not believed to be legitimate from using a service. It is also impossible to see the allegations here as stating that Comcast intentionally accesses a computer without authorization. Unless these computers operate in non-standard ways, the initiation of access is laid at e360's door, not at Comcast's.

law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle or store certain types of electronic mail messages.” See *White Buffalo Ventures, LLC v. University of Texas*, 420 F.3d 366, 371 (5th Cir. 2005); § 7707(c).

Under the law, a mistaken choice to block, if made in good faith, cannot be the basis for liability under federal or state law. To force a provider like Comcast to litigate the question of whether what it blocked was or was not spam would render § 230(c)(2) nearly meaningless.

What is left for e360 is to claim that Comcast has not acted in good faith. It argues that claim in this way: “Comcast has not acted in good faith. Comcast allows numerous other companies to send bulk emails in greater volume and with greater frequency . . . singling out Plaintiff when others behaving in a like manner are not treated in a like fashion.” Pl.’s Resp. to Def.’s Mot. for J. on the Pleadings.<sup>3</sup>

---

<sup>3</sup>Comcast argues that, absent its statutory protection, e360 has failed to state claims on all of its Counts.

(A) I agree that the Tortious Interference with Prospective Economic Advantage Count is difficult to understand. I have found no cases in which refusal to allow a plaintiff to run an advertisement in a medium with wide circulation (and thus reducing sales) of plaintiff’s products or those from whom he is selling constitutes such tortious interference. Usually the prospective economic advantage is far more concrete than selling to public which consists of people on a very, very long opt-in list. It is illegal to interfere with a fair number of prospects, but usually they are a class of easily identified individuals and usually the interference is that of the defendant interacting directly with the prospective buyers.

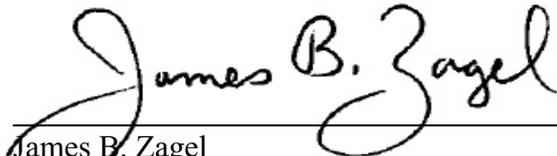
(B) The claim under CFAA under the “denial of service” theory fails for the reasons stated above.

(C) Comcast is a private enterprise and has no obligation to honor the free speech rights of e360. *C.B.S. v. Democratic Nat’l Comm.*, 412 U.S. 94 (1973). Comcast provides services traditionally performed by private enterprises, not the government. The government does not, with very few exceptions, connect people with one another through the Internet. *Jackson v. Metropolitan Edison*, 419 U.S. 345 (1974) (publicly regulated utility). The fact that an enterprise is regulated, licensed, or funded by the government does not make the enterprise part of the state. *Wilcher v. City of Akron*, 498 F.3d 516 (6th Cir. 2007).

The issue is whether e360 has pled an absence of good faith. Under the standards of *Bell Atlantic Corp. v. Twombly*, 127 S.Ct. 1955 (2007), e360 has not done so. The affidavit of the President of e360 does not attest to Comcast's alleged policy of allowing others to do what it denies e360. And Comcast does not claim that the reason it refuses to transmit e360's electronic mails is their volume and their frequency. The absence of good faith is not adequately pled.

I grant judgment on the pleadings with respect to the complaint as a whole on the grounds that § 230(c) precludes proceeding on any of the claims. Alternatively, I dismiss the remainder of the claims for the reasons stated above.

ENTER:

  
\_\_\_\_\_  
James B. Zagel  
United States District Judge

DATE: April 10, 2008

---

(D) The state law claim for unfair competition is weightless. Comcast did not deceive e360 since Comcast told e360 that Comcast reserved the right to refuse service, besides which e360 is not a consumer under Illinois law.